

# NICHOLS ALGEBRAS OF GROUP TYPE WITH MANY QUADRATIC RELATIONS

M. GRAÑA, I. HECKENBERGER, AND L. VENDRAMIN

**ABSTRACT.** We classify Nichols algebras of irreducible Yetter-Drinfeld modules over nonabelian groups satisfying an inequality for the dimension of the homogeneous subspace of degree two. All such Nichols algebras are finite-dimensional, and all known finite-dimensional Nichols algebras of nonabelian group type appear in the result of our classification. We find a new finite-dimensional Nichols algebra over fields of characteristic two.

## 1. INTRODUCTION

In many mathematical theories the classification of fundamental objects is a central and difficult problem. Successful classifications like the one of finite Coxeter groups, finite simple groups, and finite-dimensional simple Lie algebras serve as archetype for other theories. Often a finiteness assumption is imposed to achieve a reasonable result.

The theory of Hopf algebras covers classes of examples like group algebras, enveloping algebras of Lie algebras, regular functions on finite and affine algebraic groups, quantum groups and others. Additionally, many examples admit various kinds of deformations. With the discovery of quantum groups by Drinfeld and Jimbo [9, 18] it became clear that non-commutative and non-cocommutative Hopf algebras are natural objects playing an important role in many mathematical and physical theories. The large variety of examples forces any classification ansatz to restrict oneself to a special class.

A Hopf algebra is *pointed* if all irreducible subcomodules are one-dimensional. Examples of pointed Hopf algebras are universal enveloping algebras of Lie algebras and restricted Lie algebras and quantized enveloping algebras. The first non-commutative non-cocommutative examples have been the Sweedler Hopf algebra [23] and the Taft Hopf algebra [24]. A systematic study of pointed Hopf algebras was started by Nichols [21]. The classification enjoyed significant progress with the invention of the lifting method by Andruskiewitsch and Schneider [3]. The idea of the method is to understand first the coradically graded Hopf algebras and then to lift them to non-graded Hopf algebras. Coradically graded pointed Hopf algebras are biproducts (bosonizations) of a group algebra and a graded braided Hopf algebra with primitives concentrated in degree one. The latter is a *Nichols algebra* if it is generated by the elements of degree one. The subspace of primitives is a *Yetter-Drinfeld module* over the group algebra and determines the Nichols algebra uniquely. Based on the lifting method, Andruskiewitsch and Schneider [5] classified finite-dimensional pointed Hopf algebras with abelian coradical under the assumption that the order of any group-like element is relatively prime to 2, 3, 5,

and 7. The proof of this remarkable result makes heavily use of the classification of Nichols algebras of diagonal type [16, 17].

The next natural step in the classification of pointed Hopf algebras is to ask for finite-dimensional Nichols algebras over nonabelian groups. This problem turns out to be extremely difficult. So far only a small number of examples appeared in the literature, and there is no obvious way to describe them in a unified way. Fomin and Kirillov [10] studied Nichols algebras over symmetric groups and they used them to analyze the geometry of Schubert cells. These and other examples have been found independently by Milinski and Schneider [20]. Andruskiewitsch and the first author investigated Nichols algebras in terms of racks and detected yet another examples [2]. At the moment, the calculation of the Hilbert series of these algebras requires the use of computer algebra. In general, the lack of knowledge about the general structure of Nichols algebras does not allow to decide if a given Nichols algebra is finite-dimensional.

In this paper we introduce a condition on the Nichols algebra in form of an inequality concerning the dimension of the degree two subspace. Our goal is to classify Nichols algebras of irreducible Yetter-Drinfeld modules over nonabelian groups under this assumption. Our main result is Theorem 4.14 which states that all such Nichols algebras are finite-dimensional, and all known examples appear this way. We recall the list of examples in Table 1. Our approach is very general and does not need any assumption on the base field. It relies heavily on our Theorem 2.37 which is a classification of racks satisfying certain inequality. With Theorem 4.4 we present a method to compare Nichols algebras defined over different fields. By consequent application of our theory it was possible to find a substantially new example of a finite-dimensional Nichols algebra over fields of characteristic 2, see Proposition 5.7.

TABLE 1. Finite-dimensional Nichols algebras

Rank	Dimension	Hilbert series	Remark
3	12	$(2)_t^2(3)_t$	Prop. 5.4
4	36	$(2)_t^2(3)_t^2$	Prop. 5.6(3), $\text{char } \mathbb{k} = 2$
4	72	$(2)_t^2(3)_t(6)_t$	Prop. 5.6(2), $\text{char } \mathbb{k} \neq 2$
5	1280	$(4)_t^4(5)_t$	Prop. 5.15(2)
5	1280	$(4)_t^4(5)_t$	Prop. 5.15(2)
6	576	$(2)_t^2(3)_t^2(4)_t^2$	Prop. 5.9
6	576	$(2)_t^2(3)_t^2(4)_t^2$	Prop. 5.11
7	326592	$(6)_t^6(7)_t$	Prop. 5.15(3)
7	326592	$(6)_t^6(7)_t$	Prop. 5.15(3)
10	8294400	$(4)_t^4(5)_t^2(6)_t^4$	Prop. 5.13
10	8294400	$(4)_t^4(5)_t^2(6)_t^4$	Prop. 5.13

## 2. RACKS

**2.1. Generalities.** A *rack* is a pair  $(X, \triangleright)$ , where  $X$  is a non-empty set and  $\triangleright : X \times X \rightarrow X$  is a map (considered as a binary operation on  $X$ ) such that

- (R1) the map  $\varphi_i : X \rightarrow X$ , where  $x \mapsto i \triangleright x$ , is bijective for all  $i \in X$ , and
- (R2)  $i \triangleright (j \triangleright k) = (i \triangleright j) \triangleright (i \triangleright k)$  for all  $i, j, k \in X$ .

A rack  $(X, \triangleright)$ , or shortly  $X$ , is a *quandle* if  $i \triangleright i = i$  for all  $i \in X$ .

The *inner group* of a rack  $X$  is the group generated by the permutations  $\varphi_i$  of  $X$ , where  $i \in X$ . We write  $\text{Inn}(X)$  for the inner group of  $X$ . Axiom (R2) implies that

$$(2.1) \quad \varphi_{i \triangleright j} = \varphi_i \varphi_j \varphi_i^{-1}$$

for all  $i, j \in X$ . More generally, the following holds.

**Lemma 2.1.** *Let  $X$  be a rack and let  $k \in \mathbb{N}_0$  and  $i_1, i_2, \dots, i_k, j, l \in X$  such that  $\varphi_{i_1} \varphi_{i_2} \cdots \varphi_{i_k}(j) = l$ . Then  $\varphi_{i_1} \varphi_{i_2} \cdots \varphi_{i_k} \varphi_j \varphi_{i_k}^{-1} \cdots \varphi_{i_2}^{-1} \varphi_{i_1}^{-1} = \varphi_l$ .*

*Proof.* By induction on  $k$  using Equation (2.1).  $\square$

A *subrack* of a rack  $X$  is a non-empty subset  $Y \subseteq X$  such that  $(Y, \triangleright)$  is also a rack. We say that a rack  $X$  is *indecomposable* if the inner group  $\text{Inn}(X)$  acts transitively on  $X$ . Also,  $X$  is *decomposable* if it is not indecomposable.

Let  $(X, \triangleright)$  and  $(Y, \triangleright)$  be racks. A map  $f : (X, \triangleright) \rightarrow (Y, \triangleright)$  is a *morphism* of racks if  $f(i \triangleright j) = f(i) \triangleright f(j)$ , for all  $i, j \in X$ .

**Example 2.2.** A group  $G$  is a rack with  $x \triangleright y = xyx^{-1}$  for all  $x, y \in G$ . If a subset  $X \subseteq G$  is stable under conjugation by  $G$ , then it is a subrack of  $G$ . In particular, we list the following examples.

- (1) The rack given by the conjugacy class of involutions in  $G = \mathbb{D}_p$ , the dihedral group with  $2p$  elements, has  $p$  elements. It is called the *dihedral rack* (of order  $p$ ) and will be denoted by  $\mathbb{D}_p$ .
- (2) Let  $\mathcal{T}$  be the conjugacy class of  $(2\ 3\ 4)$  in  $\mathbb{A}_4$ . We use the following labeling for the elements of  $\mathcal{T}$ :  $\pi_1 = (2\ 3\ 4)$ ,  $\pi_2 = (1\ 4\ 3)$ ,  $\pi_3 = (1\ 2\ 4)$ ,  $\pi_4 = (1\ 3\ 2)$ . This is the rack associated with the vertices of the tetrahedron.
- (3) Let  $\mathcal{A}$  be the conjugacy class of  $(1\ 2)$  in  $\mathbb{S}_4$ . We use the following labeling for the elements of  $\mathcal{A}$ :  $\pi_1 = (3\ 4)$ ,  $\pi_2 = (2\ 3)$ ,  $\pi_3 = (2\ 4)$ ,  $\pi_4 = (1\ 2)$ ,  $\pi_5 = (1\ 3)$ ,  $\pi_6 = (1\ 4)$ .
- (4) Let  $\mathcal{B}$  be the rack given by the permutations  $\varphi_1 = (2\ 3\ 4\ 5)$ ,  $\varphi_2 = (1\ 5\ 6\ 3)$ ,  $\varphi_3 = (1\ 2\ 6\ 4)$ ,  $\varphi_4 = (1\ 3\ 6\ 5)$ ,  $\varphi_5 = (1\ 4\ 6\ 2)$ ,  $\varphi_6 = (2\ 5\ 4\ 3)$ . This rack can be realized as the conjugacy class of 4-cycles in  $\mathbb{S}_4$ . The rack  $\mathcal{B}$  is not isomorphic to  $\mathcal{A}$ . Indeed, for all  $i \in \mathcal{A}$  the map  $\varphi_i \in \text{Inn}(\mathcal{A})$  is an involution, but  $1 \triangleright (1 \triangleright 2) = 4$  in  $\mathcal{B}$ .
- (5) Let  $\mathcal{C}$  be the conjugacy class of  $(1\ 2)$  in  $\mathbb{S}_5$ . We use the following labeling for the elements of  $\mathcal{C}$ :  $\pi_1 = (1\ 2)$ ,  $\pi_2 = (2\ 3)$ ,  $\pi_3 = (1\ 3)$ ,  $\pi_4 = (2\ 4)$ ,  $\pi_5 = (1\ 4)$ ,  $\pi_6 = (2\ 5)$ ,  $\pi_7 = (1\ 5)$ ,  $\pi_8 = (3\ 4)$ ,  $\pi_9 = (3\ 5)$ ,  $\pi_{10} = (4\ 5)$ .

**Example 2.3.** Let  $p$  be a prime number and let  $q$  be a power of  $p$ . Let  $X = \mathbb{F}_q$ , the finite field of  $q$  elements. For  $0 \neq \alpha \in \mathbb{F}_q$  we have a rack structure on  $X$  given by  $x \triangleright y = (1 - \alpha)x + \alpha y$  for all  $x, y \in X$ . This rack is called the *affine rack* associated to the pair  $(\mathbb{F}_q, \alpha)$  and will be denoted by  $\text{Aff}(q, \alpha)$ . These racks are also called Alexander quandles, see [7].

*Remark 2.4.* Let  $X$  be a finite rack and assume that  $\text{Inn}(X)$  acts transitively on  $X$ . Then for all  $i, j \in X$  there exist  $r \in \mathbb{N}_0$  and  $k_1, k_2, \dots, k_r \in X$  such that  $\varphi_{k_1}^{\pm 1} \varphi_{k_2}^{\pm 1} \cdots \varphi_{k_r}^{\pm 1}(i) = j$ . Lemma 2.1 implies that all permutations  $\varphi_i$ , where  $i \in X$ , have the same cycle structure.

**Lemma 2.5.** *Let  $X$  be a finite rack, and let  $Y$  be a non-empty proper subset of  $X$ . The following are equivalent.*

- (1)  $X = Y \cup (X \setminus Y)$  is a decomposition of  $X$ .
- (2)  $X \triangleright Y \subseteq Y$ .

*Proof.* See [2, Lemma 1.14].  $\square$

**Lemma 2.6.** *Let  $X$  be a rack and let  $a, x, y, z \in X$  such that  $x \triangleright y = z$ ,  $a \triangleright x = x$  and  $a \triangleright z = z$ . Then  $a \triangleright y = y$ .*

*Proof.* We have  $x \triangleright y = z = a \triangleright z = a \triangleright (x \triangleright y) = (a \triangleright x) \triangleright (a \triangleright y) = x \triangleright (a \triangleright y)$ . Thus the claim follows from (R1).  $\square$

**Lemma 2.7.** *Let  $X$  be a rack and let  $a, b, c, d \in X$  such that  $a \triangleright a = a$ . If  $a \triangleright c = b \triangleright c$ ,  $a \triangleright d = b \triangleright d$  and  $c \triangleright d = a$  then  $b \triangleright a = a$ .*

*Proof.*  $b \triangleright a = b \triangleright (c \triangleright d) = (b \triangleright c) \triangleright (b \triangleright d) = (a \triangleright c) \triangleright (a \triangleright d) = a \triangleright (c \triangleright d) = a \triangleright a = a$ .  $\square$

We say that a rack is *involutive* if  $\varphi_i$  is an involution for every  $i \in X$ , that is, if  $i \triangleright (i \triangleright j) = j$  for every  $i, j \in X$ . The dihedral racks and the racks  $\mathcal{A}$  and  $\mathcal{C}$  of Example 2.2 are involutive.

**Lemma 2.8.** *Let  $X$  be an involutive rack. Let  $a, b, c \in X$  such that  $a \triangleright a = a$ . If  $b \triangleright a = c \triangleright a$  and  $a \triangleright b = c \triangleright b$  then  $a \triangleright (b \triangleright a) = b \triangleright a$ .*

*Proof.*  $a \triangleright (b \triangleright a) = (a \triangleright b) \triangleright (a \triangleright a) = (c \triangleright b) \triangleright a = c \triangleright (b \triangleright (c \triangleright a)) = c \triangleright a = b \triangleright a$ .  $\square$

**2.2. The enveloping group of a rack.** For any rack  $X$ , the *enveloping group* of  $X$  is

$$G_X = F(X) / \langle iji^{-1} = i \triangleright j, i, j \in X \rangle,$$

where  $F(X)$  denotes the free group generated by  $X$ . We write  $Z(G_X)$  for the center of  $G_X$ . For all  $i \in X$  let  $x_i$  be the image of  $i$  under  $X \hookrightarrow F(X) \rightarrow G_X$ .

*Remark 2.9.* The enveloping group  $G_X$  of a rack  $X$  is  $\mathbb{Z}$ -graded by  $\deg x_i = 1$  for all  $i \in X$ .

A rack  $X$  is *faithful* if the map  $X \rightarrow \text{Inn}(X)$  defined by  $i \mapsto \varphi_i$  is injective, see [2, Def. 1.11]. A rack  $X$  is *injective* if the map  $X \rightarrow G_X$  defined by  $i \mapsto x_i$  is injective, see [22, Def. 8].

**Lemma 2.10.** *Any faithful rack is injective.*

*Proof.* Let  $X$  be a faithful rack and let  $i, j \in X$ . By (R1), (R2) and the definition of  $G_X$  the group  $G_X$  acts on  $X$  such that  $x_k \triangleright l = k \triangleright l$  for all  $k, l \in X$ . If  $i \neq j$  then  $\varphi_i \neq \varphi_j$  since  $X$  is faithful. Hence there exists  $k \in X$  such that  $x_i \triangleright k = i \triangleright k \neq j \triangleright k = x_j \triangleright k$ . It follows that  $x_i \neq x_j$  in  $G_X$  and hence  $X$  is injective.  $\square$

**Example 2.11.** We give a rack which is not injective. Let  $X = \{1, 2, 3\}$  and  $\triangleright : X \times X \rightarrow X$  the map with  $1 \triangleright i = 2 \triangleright i = i$  for all  $i \in X$  and  $3 \triangleright 1 = 2$ ,  $3 \triangleright 2 = 1$ ,  $3 \triangleright 3 = 3$ . Then  $X$  is a rack (and even a quandle). In  $G_X$  the relations  $x_1 x_3 x_1^{-1} = x_3$  and  $x_3 x_1 x_3^{-1} = x_2$  hold and hence  $x_1 x_3 = x_3 x_1 = x_2 x_3$ . Thus  $x_1 = x_2$  in  $G_X$ , that is,  $X$  is not injective.

**Example 2.12.** We give a rack which is injective but not faithful. Let  $X = \{1, 2\}$  and  $\triangleright : X \times X \rightarrow X$  the map with  $i \triangleright j = j$  for all  $i, j \in X$ . Then  $\text{Inn}(X)$  is trivial and  $G_X \cong \mathbb{Z}^2$ . We conclude that  $X$  is injective but not faithful.

**Lemma 2.13.** *Let  $X$  be a rack and let  $k \in \mathbb{N}_0$ ,  $i_1, \dots, i_k, l \in X$ , and  $\epsilon_1, \dots, \epsilon_k \in \{1, -1\}$ . If  $l$  is a fixed point of the permutation  $\varphi_{i_1}^{\epsilon_1} \varphi_{i_2}^{\epsilon_2} \dots \varphi_{i_k}^{\epsilon_k}$  then  $x_{i_1}^{\epsilon_1} x_{i_2}^{\epsilon_2} \dots x_{i_k}^{\epsilon_k}$  belongs to the centralizer of  $x_l$  in  $G_X$ . The converse is true if  $X$  is injective.*

*Proof.* Since  $x_i x_j = x_{i \triangleright j} x_i$  for all  $i, j \in X$ , we have

$$(2.2) \quad (x_{i_1} x_{i_2} \dots x_{i_k}) x_l = x_{i_1 \triangleright (i_2 \triangleright \dots \triangleright (i_k \triangleright l))} (x_{i_1} x_{i_2} \dots x_{i_k})$$

and the result follows if  $\epsilon_i = 1$  for all  $i$ . The general case is similar.  $\square$

**Corollary 2.14.** *Let  $X$  be a rack and let  $k \in \mathbb{N}_0$ ,  $i_1, \dots, i_k, l \in X$ , and  $\epsilon_1, \dots, \epsilon_k \in \{1, -1\}$ . If  $\varphi_{i_1}^{\epsilon_1} \varphi_{i_2}^{\epsilon_2} \dots \varphi_{i_k}^{\epsilon_k} = \text{id}$  then  $x_{i_1}^{\epsilon_1} x_{i_2}^{\epsilon_2} \dots x_{i_k}^{\epsilon_k}$  is central in  $G_X$ . The converse is true if  $X$  is injective.*

The following result is a special case of [2, Lemma 1.9(2)].

**Corollary 2.15.** *Let  $X$  be an injective rack. Then  $\text{Inn}(X) \simeq G_X / Z(G_X)$ .*

Corollary 2.15 fails without the assumption that  $X$  is injective. Indeed, in Example 2.11 the group  $G_X$  is abelian but  $\text{Inn}(X)$  is not the trivial group.

For the rest of Subsection 2.2 let  $X$  be a finite rack. For all  $i, j \in X$  and  $n \in \mathbb{N}$  we define  $i \triangleright^n j = \varphi_i^n(j)$ .

**Lemma 2.16.** *Let  $n \in \mathbb{N}_0$  and let  $i, j \in X$ .*

- (1)  $x_i^n x_j = x_{i \triangleright^n j} x_i^n$ .
- (2)  $x_i x_j^n = x_{i \triangleright j} x_i^n$ .

*Proof.* By induction on  $n$ .  $\square$

**Lemma 2.17.** *Let  $i \in X$  and let  $n$  be the order of  $\varphi_i$ . Then  $x_i^n \in Z(G_X)$ .*

*Proof.* Follows from Lemma 2.16(1).  $\square$

**Lemma 2.18.** *Assume that  $X$  is indecomposable. Then all permutations  $\varphi_i$ , where  $i \in X$ , have the same order  $n$ . Moreover,  $x_i^n = x_j^n$  for all  $i, j \in X$ .*

*Proof.* Since  $X$  is indecomposable, the first claim follows from Equation (2.1). The second claim holds by Lemmas 2.16(2) and 2.17.  $\square$

For the rest of Subsection 2.2 assume that  $X$  is (finite and) indecomposable. Let  $d$  denote the number of elements of  $X$ . For convenience we identify  $X$  with  $\{1, 2, \dots, d\}$ . Let  $n$  be the order of  $\varphi_1$ . Lemma 2.17 implies that the subgroup  $\langle x_1^n \rangle$  of  $G_X$  generated by  $x_1^n$  is normal in  $G_X$ . Let

$$\overline{G_X} = G_X / \langle x_1^n \rangle$$

and let  $\pi : G_X \rightarrow \overline{G_X}$  be the canonical projection.

**Lemma 2.19.** *The group  $\overline{G_X}$  is finite.*

*Proof.* First we prove that for all  $i, j \in X$  with  $i \neq j$  there exist  $k, l \in X$  such that  $x_k x_l = x_i x_j$ ,  $k < l$  and  $(k, l)$  is lexicographically not bigger than  $(i, j)$ . If  $i < j$  then the claim is trivial. Assume that  $i > j$ . Then  $x_i x_j = x_j x_k$ , where  $k \in X$  with  $j \triangleright k = i$ . Since  $(j, k)$  is lexicographically smaller than  $(i, j)$ , the claim follows by induction on  $i$ .

By Lemmas 2.17 and 2.18 all elements of  $G_X$  take the form  $x_{i_1} \dots x_{i_k} x_1^{tn}$  for some  $k \in \mathbb{N}_0$ ,  $i_1, \dots, i_k \in X$  and  $t \in \mathbb{Z}$ . By the first paragraph of the proof we may assume that  $i_1 \leq i_2 \leq \dots \leq i_k$  and by Lemmas 2.17 and 2.18 we may assume that at most  $n - 1$  consecutive  $x_{i_j}$  are equal. This implies the claim.  $\square$

**Lemma 2.20.** *The following hold.*

- (1)  $C_{G_X}(x_1) = \pi^{-1}C_{\overline{G_X}}(\pi x_1)$ .
- (2) *If  $C_{\overline{G_X}}(\pi x_1)$  is abelian then  $C_{G_X}(x_1)$  is abelian.*
- (3) *If  $C_{\overline{G_X}}(\pi x_1)$  is cyclic and generated by  $\pi x_1$  then  $C_{G_X}(x_1)$  is cyclic and generated by  $x_1$ .*

*Proof.* (1) The inclusion  $\subseteq$  is trivial. Let  $\bar{z} \in C_{\overline{G_X}}(\pi x_1)$  and let  $z \in G_X$  such that  $\pi z = \bar{z}$ . Then  $\pi z = \pi(x_1 z x_1^{-1})$ . This implies that  $x_1 z x_1^{-1} = z x_1^{nm}$  for some  $m \in \mathbb{Z}$ . Since  $G_X$  is  $\mathbb{Z}$ -graded, see Remark 2.9, it follows that  $m = 0$ . Hence  $z \in C_{G_X}(x_1)$ .

(2) Let  $x, y \in C_{G_X}(x_1)$ . Then  $\pi(xy x^{-1}) = \pi y$  since  $C_{\overline{G_X}}(\pi x_1)$  is abelian. Hence  $xy x^{-1} = y x_1^{nm}$  for some  $m \in \mathbb{Z}$ . Moreover  $m = 0$  since  $G_X$  is  $\mathbb{Z}$ -graded. Thus (2) holds.

(3) Let  $y \in C_{G_X}(x_1)$ . Then  $\pi y \in C_{\overline{G_X}}(\pi x_1)$ , and hence  $\pi y = (\pi x_1)^p$  for some  $p \in \mathbb{Z}$  by assumption. Therefore  $y = x_1^{p+nm}$  for some  $m \in \mathbb{Z}$ .  $\square$

*Remark 2.21.* Lemma 2.20(1) is a particular case of a more general fact. Let  $p : H \rightarrow G$  be an epimorphism of groups and let  $h \in H$  such that the restriction of  $p$  to the conjugacy class of  $h$  in  $H$  is injective. Then  $p^{-1}C_G(ph) = C_H(h)$ . Indeed, the inclusion  $\supseteq$  is trivial. Moreover, if  $g \in H$  such that  $(pg)(ph)(pg)^{-1} = (ph)$  then  $ghg^{-1} = h$  by the assumption on  $p$ .

**2.3. Braided action.** Let  $G$  be a group. Let  $X$  be a conjugacy class of  $G$ , viewed as a rack with  $x \triangleright y = xyx^{-1}$  for all  $x, y \in X$ . Assume that  $G$  is generated by  $X$ . Then  $X$  is an indecomposable rack by Lemma 2.5. Moreover  $X$  is injective by definition. Let  $d = \#X$ . In what follows we assume that  $X = \{x_1, x_2, \dots, x_d\}$  is finite and that  $d > 1$ . When considering  $X$  as a rack, we write  $i$  for  $x_i$ .

*Remark 2.22.* The rack  $X$  satisfies the following.

- (1)  $i \triangleright i = i$  for all  $i \in X$ .
- (2) For all  $i, j \in X$  we have  $i \triangleright j = j$  if and only if  $j \triangleright i = i$ .

A rack satisfying properties (1) and (2) is called a *crossed set*.

The following lemma will be used as an indecomposability criterion.

**Lemma 2.23.** *Let  $Y$  be a finite crossed set which is indecomposable as a rack. Let  $y \in Y$ , and let  $n$  be the number of elements of  $Y$  not fixed by  $\varphi_y$ . Let  $Y_1, Y_2 \subseteq Y$  such that  $Y_1 \neq \emptyset$  and that the following hold.*

- (1)  $y_1 \triangleright z = z$  for all  $y_1 \in Y_1, z \in Y \setminus Y_2$ .
- (2) For all  $y_2 \in Y_2$  there exist  $n$  elements of  $Y_1$  not commuting with  $y_2$ .

*Then  $Y_1 = Y_2 = Y$ .*

*Proof.* Since  $Y$  is indecomposable, the number  $n$  is independent of the choice of  $y \in Y$ . Since  $Y$  is a crossed set, Remark 2.22(2) and the definition of  $n$  imply that  $y_2 \triangleright Y_1 = Y_1$  for all  $y_2 \in Y_2$ . Further,  $z \triangleright Y_1 = Y_1$  for all  $z \in Y \setminus Y_2$  by (1) and by Remark 2.22(2). Hence  $Y = Y_1$  by Lemma 2.5 and since  $Y_1 \neq \emptyset$ . Since  $Y$  is indecomposable, assumption (1) and Lemma 2.5 imply that  $Y_2 = Y$ .  $\square$

Let  $c : X \times X \rightarrow X \times X$  be defined by  $c(i, j) = (i \triangleright j, i)$ . The map  $c$  is a solution of the braid equation. Since  $X$  is finite, we have  $c^n = \text{id}$  for some  $n \in \mathbb{N}_0$  with  $n \geq 1$ . Let  $H$  be the group generated by  $c$ . The group  $H$  acts on  $X \times X$  and the orbits of this action are  $\mathcal{O}(i, j) = \{c^m(i, j) \mid m \in \mathbb{Z}\}$ , where  $(i, j) \in X \times X$ .

*Remark 2.24.* The group  $G$  acts by conjugation on  $X$ . Also,  $G$  acts on  $X \times X$  diagonally:  $g \triangleright (x, y) = (g \triangleright x, g \triangleright y)$  for all  $g \in G$  and  $x, y \in X$ . For all  $g \in G$  and all  $x, y \in X$  we have  $\mathcal{O}(g \triangleright x, g \triangleright y) = g \triangleright \mathcal{O}(x, y)$ . In particular, for all  $i, j \in X$  the sets  $\mathcal{O}(i, i \triangleright j)$  and  $\mathcal{O}(j \triangleright i, j)$  have the same cardinality as  $\mathcal{O}(i, j)$ . By definition we obtain that  $\#\mathcal{O}(i, j) = 1$  if and only if  $i = j$ . Similarly,  $\#\mathcal{O}(i, j) = 2$  if and only if  $i \neq j$  and  $x_i$  and  $x_j$  commute (i.e.  $i \triangleright j = j$ ).

The set  $X \times X$  is the disjoint union of the orbits under the action of  $H$ . For all  $n \in \mathbb{N}_0$  let

$$l_n = \#\{\mathcal{O}(i, j) : \mathcal{O}(i, j) \text{ has } n \text{ elements}\}.$$

Since  $l_1 = d$ , we obtain that

$$(2.3) \quad d + 2l_2 + 3l_3 + \cdots = d^2.$$

For all  $n \in \mathbb{N}_0$  let

$$k_n = \#\{j \in X \mid \#\mathcal{O}(1, j) = n\}.$$

Remark 2.24 implies that

$$k_n = \#\{j \in X \mid \#\mathcal{O}(i, j) = n\}$$

for all  $i \in X$  and all  $n \in \mathbb{N}_0$ .

**Lemma 2.25.** *The rack  $X$  has the following properties.*

- (1) Let  $i, j, k \in X$ . If  $\mathcal{O}(i, j) = \mathcal{O}(i, k)$  then  $j = k$ . If  $\mathcal{O}(i, j) = \mathcal{O}(k, j)$  then  $i = k$ .
- (2) For all  $i, j \in X$  we have  $\#\mathcal{O}(i, j) \leq d$ . In particular,  $d \geq n$  for all  $n \in \mathbb{N}_0$  with  $k_n \geq 1$ .
- (3) For all  $i \in X$  the permutation  $\varphi_i$  has precisely  $k_2 + 1$  fixed points. In particular, if  $k_2 = d - 1$  then  $X$  is trivial (i.e.  $i \triangleright j = j$  for all  $i, j \in X$ ).
- (4)  $1 + k_2 + k_3 + \cdots = d$ .

*Proof.* (1) Since  $c(i, j) = (i \triangleright j, i) = (x_i x_j x_i^{-1}, x_i)$  and  $x_i x_j = (x_i x_j x_i^{-1}) x_i$  in  $G$ , it follows that  $x_i x_j = x_l x_m$  for all  $(l, m) \in \mathcal{O}(i, j)$ . In particular, if  $(i, k) \in \mathcal{O}(i, j)$  then  $x_i x_k = x_i x_j$  and hence  $j = k$ . Similarly, if  $\mathcal{O}(i, j) = \mathcal{O}(k, j)$  then  $x_i x_j = x_k x_j$  and hence  $i = k$ .

(2) follows from (1).

(3) Let  $i, j \in X$ . Then  $j$  is a fixed point of  $\varphi_i$  if and only if  $i = j$  or  $\mathcal{O}(i, j)$  has size 2. This gives the claim.

(4) By (1) the orbits  $\mathcal{O}(1, i)$  with  $1 \leq i \leq d$  are disjoint. Since  $\#\mathcal{O}(1, 1) = 1$  and  $2 \leq \#\mathcal{O}(1, i) < \infty$  for all  $i \geq 2$ , the claim follows.  $\square$

**Lemma 2.26.** *For all  $n \in \mathbb{N}_0$  we have  $l_n = \frac{dk_n}{n}$ .*

*Proof.* Let  $n \in \mathbb{N}_0$  and let  $\Gamma_n = \{(i, j) \in X \times X \mid \#\mathcal{O}(i, j) = n\}$ . The set  $\Gamma_n$  is invariant under the action of  $H$ , and every  $H$ -orbit of  $\Gamma_n$  has size  $n$  by definition of  $\Gamma_n$ . Hence  $\#\Gamma_n = nl_n$ . On the other hand,  $\Gamma_n$  is invariant under the diagonal action of  $G$  by Remark 2.24. Since  $G$  acts transitively on  $X$ , we conclude that every  $G$ -orbit of  $\Gamma_n$  has size  $d$  and contains a unique element  $(1, j)$ , where  $j \in X$ . Hence  $\#\Gamma_n = dk_n$ . Therefore  $nl_n = dk_n$ .  $\square$



Let  $x, y \in X$ . For all  $n \in \mathbb{N}_0$  define recursively  $a_n, b_n \in X$  by

$$\begin{aligned} a_0 &= x, & b_0 &= y \\ a_1 &= x \triangleright y, & b_1 &= y \triangleright x \\ a_{n+1} &= a_n \triangleright a_{n-1}, & b_{n+1} &= b_n \triangleright b_{n-1}, \quad n \geq 1. \end{aligned}$$

**Lemma 2.27.** *Let  $x, y \in X$  and  $n \in \mathbb{N}_0$  with  $n \geq 1$ . Then the following hold.*

- (1)  $c^n(x, y) = (a_n, a_{n-1})$ .
- (2)  $a_n = x \triangleright b_{n-1}$ .
- (3)  $b_n = y \triangleright a_{n-1}$ .

*Proof.* (1) follows by induction on  $n$  from the definition of  $c$ , and (3) is obtained from (2) by exchanging  $x$  and  $y$ . We prove (2) by induction on  $n$ . The case  $n = 1$  is trivial. The induction step follows from the equations

$$x \triangleright b_n = x \triangleright (b_{n-1} \triangleright b_{n-2}) = (x \triangleright b_{n-1}) \triangleright (x \triangleright b_{n-2}) = a_n \triangleright a_{n-1} = a_{n+1}$$

which are obtained from Axiom (R2) and the induction hypothesis.  $\square$

*Notation 2.28.* We write  $x \blacktriangleright_n y = a_{n-1}$  and  $y \blacktriangleright_n x = b_{n-1}$  for all  $n \in \mathbb{N}_0$  with  $n \geq 1$ . By Lemma 2.27(2),(3) we obtain that

$$(2.4) \quad x \blacktriangleright_n y = \underbrace{x \triangleright (y \triangleright (x \cdots))}_{n \text{ elements of } X}.$$

For example we have

$$\begin{aligned} x \blacktriangleright_1 y &= x, & x \blacktriangleright_2 y &= x \triangleright y, \\ x \blacktriangleright_3 y &= x \triangleright (y \triangleright x), & x \blacktriangleright_4 y &= x \triangleright (y \triangleright (x \triangleright y)). \end{aligned}$$

For any  $x, y \in X$  the orbit  $\mathcal{O}(x, y)$  will also be denoted by  $[x]$  if  $x = y$  and by

$$[a_{m-2} \cdots a_2 a_1 x y]$$

if  $x \neq y$ , where  $m \geq 2$  is the smallest integer with  $c^m(x, y) = (x, y)$ . Lemma 2.27 implies that

$$(2.5) \quad [a_{m-2} \cdots a_2 a_1 x y] = [y a_{m-2} a_{m-3} \cdots a_2 a_1 x]$$

and that the elements of  $\mathcal{O}(x, y)$  with  $x \neq y$  are just the pairs  $(i, j)$  such that  $i$  and  $j$  are consecutive entries in  $[\cdots x y]$  or its cyclic permutation.

**Lemma 2.29.** *Assume that  $X$  is involutive. Let  $n \in \mathbb{N}_0$  with  $n \geq 2$  and let  $i_1, \dots, i_n \in X$  be pairwise distinct elements such that  $\mathcal{O}(i_2, i_1) = [i_n \cdots i_3 i_2 i_1]$ . Then  $\mathcal{O}(i_1, i_2) = [i_1 i_2 i_3 \cdots i_n]$ .*

*Proof.* By assumption we have  $i_l \triangleright i_{l-1} = i_{l+1}$  and  $c(i_l, i_{l-1}) = (i_{l+1}, i_l)$  for all  $l \in \{1, 2, \dots, n\}$ , where the indices are considered as elements in  $\mathbb{Z}/n\mathbb{Z}$ . Since  $X$  is involutive, it follows that  $i_l \triangleright i_{l+1} = i_{l-1}$  for all  $l \in \mathbb{Z}/n\mathbb{Z}$ . This implies the claim.  $\square$

Recall that  $G_X$  is the enveloping group of  $X$ . Since  $G$  is generated by  $X$ , there is a unique group epimorphism  $G_X \rightarrow G$  induced by the identity on  $X$ . Hence  $X$  is an injective rack. Let  $\Phi : X \rightarrow G_X$  be defined by  $x \mapsto \overline{x}$ , where  $\overline{x}$  is the coset of



$x$  in  $G_X$ . Following the notation in [12, page 7], for all  $v, w \in G_X$  and all  $n \in \mathbb{N}_0$  we write

$$\begin{aligned} \text{Prod}(v, w; 0) &= 1, & \text{Prod}(v, w; 1) &= v, & \text{Prod}(v, w; 2) &= vw, \\ \text{Prod}(v, w; n) &= \underbrace{vwvw \cdots}_{n \text{ factors}}. \end{aligned}$$

**Lemma 2.30.** *Let  $x, y \in X$ . In  $G_X$  we have*

$$\overline{x \blacktriangleright_n y} = \text{Prod}(\overline{x}, \overline{y}; n) \cdot \text{Prod}(\overline{x}, \overline{y}, n-1)^{-1}$$

for all integers  $n \geq 1$ .

*Proof.* The case  $n = 1$  is trivial. Assume now that the claim holds for  $n$ . Then

$$\begin{aligned} \Phi(x \blacktriangleright_{n+1} y) &= \Phi(x \triangleright (y \blacktriangleright_n x)) \\ &= \overline{x} \cdot \Phi(y \blacktriangleright_n x) \cdot \overline{x}^{-1} \\ &= \overline{x} \cdot \text{Prod}(y, x; n-1) \cdot \text{Prod}(y, x; n-2)^{-1} \cdot \overline{x}^{-1} \\ &= \text{Prod}(x, y; n) \cdot \text{Prod}(x, y, n-1)^{-1}. \end{aligned}$$

This completes the proof.  $\square$

**Proposition 2.31.** *Let  $x, y \in X$  and  $n \in \mathbb{N}_0$  with  $n \geq 1$ . The following are equivalent.*

- (1) *The  $H$ -orbit  $\mathcal{O}(x, y)$  has size  $n$ .*
- (2)  *$x \blacktriangleright_n y = y$  and  $x \blacktriangleright_k y \neq y$  for all  $k \in \{1, 2, \dots, n-1\}$ .*
- (3)  *$y \blacktriangleright_n x = x$  and  $y \blacktriangleright_k x \neq x$  for all  $k \in \{1, 2, \dots, n-1\}$ .*
- (4)  *$\text{Prod}(\overline{x}, \overline{y}; n) = \text{Prod}(\overline{y}, \overline{x}; n)$  and  $\text{Prod}(\overline{x}, \overline{y}; k) \neq \text{Prod}(\overline{y}, \overline{x}; k)$  for all  $k \in \{1, 2, \dots, n-1\}$ .*

*Proof.* Recall that (1) holds if and only if  $c^n(x, y) = (x, y)$  and  $c^k(x, y) \neq (x, y)$  for all  $k \in \{1, 2, \dots, n-1\}$ . Thus (1) is equivalent to (2) by Lemma 2.27(1) and Lemma 2.25(1). The equivalence between (2) and (4) follows from Lemma 2.30. Exchanging  $x$  and  $y$  in the last argument one concludes that (4) and (3) are equivalent, which finishes the proof of the proposition.  $\square$

**Corollary 2.32.** *Let  $x, y, z \in X$ . Assume that the orbit  $\mathcal{O}(x, y)$  has size 3. If  $x \triangleright y = z$  then  $y \triangleright z = x$  and  $z \triangleright x = y$ .*

**Corollary 2.33.** *Let  $x, y \in X$ . Assume that the orbit  $\mathcal{O}(x, y)$  has size 4. If  $X$  is involutive then  $x \triangleright (y \triangleright x) = y \triangleright x$  and  $y \triangleright (x \triangleright y) = x \triangleright y$ .*

Now we start to study in more detail the racks satisfying the inequality

$$(2.6) \quad d + l_2 + l_3 + \cdots \geq \frac{d(d-1)}{2}.$$

This condition is motivated by the structure of the degree two part of the Nichols algebra of  $(X, q)$ , where  $q$  is a two-cocycle, see Section 4. Our main achievement in this section will be the classification of these racks, see Theorem 2.37 below.

Lemma 2.26 and Lemma 2.25(4) imply that (2.6) is equivalent to

$$(2.7) \quad \sum_{n \geq 3} \frac{n-2}{2n} k_n \leq 1.$$

*Notation 2.34.* We write  $\mathcal{S} = \sum_{n \geq 3} \frac{n-2}{2n} k_n$ .

*Remark 2.35.* If (2.7) is satisfied, then  $k_n \leq \frac{2n}{n-2}$  for all  $n \geq 3$ . Since  $k_n \in \mathbb{Z}$  for all  $n$ , this means that  $k_3 \leq 6$ ,  $k_4 \leq 4$ ,  $k_5 \leq 3$ ,  $k_6 \leq 3$  and  $k_n \leq 2$  for all  $n > 6$ .

**Lemma 2.36.** *Let  $m = d - k_2 - 1$ . If Relation (2.7) holds then  $2 \leq m \leq 6$ .*

*Proof.* If  $k_2 = d - 1$  then  $X$  is trivial. Since  $X$  is indecomposable, this is a contradiction to  $d > 1$ . The case  $k_2 = d - 2$  is impossible by Lemma 2.25(3). Therefore  $m \geq 2$ . Relation (2.7) and Lemma 2.25(4) imply that

$$\sum_{n \geq 3} \frac{k_n}{n} \geq \sum_{n \geq 3} \frac{k_n}{2} - 1 = \frac{d - 3 - k_2}{2} = \frac{m - 2}{2}.$$

Thus

$$\frac{m - 2}{4} \leq \sum_{n \geq 3} \frac{1}{2n} k_n \leq \sum_{n \geq 3} \frac{n - 2}{2n} k_n \leq 1.$$

Therefore  $m \leq 6$ .  $\square$

**Theorem 2.37.** *Let  $G$  be a group and let  $X$  be a conjugacy class of  $G$ . Assume that  $X$  is finite and generates  $G$ . The following are equivalent.*

- (1)  $\sum_{n \geq 3} \frac{n-2}{2n} k_n \leq 1$ .
- (2) The rack  $X$  is one of the racks listed in Table 2.

*Proof.* First we prove that (1) implies (2). Since  $X$  generates  $G$ , Lemma 2.36 yields that  $k_3 + k_4 + \dots = m$ , where  $2 \leq m \leq 6$ . We split the proof in several subsections. The rack  $\mathbb{D}_3$  appears when  $m = 2$ , see Subsection 3.1. The rack  $\mathcal{T}$  appears in Subsection 3.2. The affine racks of  $\mathbb{F}_5$  (resp.  $\mathbb{F}_7$ ) appear in Subsection 3.3 (resp. 3.5). The rack  $\mathcal{B}$  appears in Subsection 3.3. The rack  $\mathcal{A}$  (resp.  $\mathcal{C}$ ) appears in Subsection 3.3 (resp. 3.5).

Now we prove that (2) implies (1). These racks are explained in Examples 2.2 and 2.3. The computations appear inside Subsections 3.1, 3.2, 3.3 and 3.5. Also, these computations can be easily done with GAP [1, 13]. It turns out that  $k_n = 0$  in all examples, where  $n > 5$ . In Table 2 we record all numbers  $k_n$  with  $2 \leq n \leq 4$ .  $\square$

TABLE 2. Racks satisfying Condition (2.7)

Rack	$d$	$k_2$	$k_3$	$k_4$	$\mathcal{S}$
$\mathbb{D}_3$	3	0	2	0	$\frac{1}{3}$
$\mathcal{T}$	4	0	3	0	$\frac{1}{2}$
Aff(5, 2)	5	0	0	4	1
Aff(5, 3)	5	0	0	4	1
$\mathcal{A}$	6	1	4	0	$\frac{2}{3}$
$\mathcal{B}$	6	1	4	0	$\frac{2}{3}$
Aff(7, 3)	7	0	6	0	1
Aff(7, 5)	7	0	6	0	1
$\mathcal{C}$	10	3	6	0	1

### 3. THE PROOF OF THEOREM 2.37

This section is devoted to the proof of Theorem 2.37.

**3.1. The case  $k_3 + k_4 + \dots = 2$ .** By Lemma 2.25(3),(4) every permutation  $\varphi_i$ , where  $i \in X$ , is a transposition. Without loss of generality we may assume that  $\varphi_1 = (23)$ . Hence  $\#\mathcal{O}(1, i) > 2$  if and only if  $i \in \{2, 3\}$ . Moreover,

$$\#\mathcal{O}(1, 3) = \#(1 \triangleright \mathcal{O}(1, 2)) = \#\mathcal{O}(1, 2)$$

by Remark 2.24. Let  $n = \#\mathcal{O}(1, 2)$ . Then

$$(3.1) \quad k_n = 2 \text{ and } k_m = 0 \text{ for all } m \geq 3, m \neq n.$$

Lemma 2.25(2) implies that  $d \geq n$ . We split the proof in three steps.

*Step 1.*  $n = 3$ . The definition of  $c$  implies that

$$\mathcal{O}(1, 2) = [3 \ 1 \ 2].$$

Hence  $\varphi_1 = (23)$ ,  $\varphi_2 = (13)$  and  $\varphi_3 = (12)$ . Thus  $X = \{1, 2, 3\}$  by Lemma 2.23 with  $Y_1 = Y_2 = \{1, 2, 3\}$ . Therefore  $X$  is the dihedral rack of 3 elements.

*Step 2.*  $n = 4$ . Corollary 2.33 with  $(x, y) = (1, 3)$  implies that  $1 \triangleright (3 \triangleright 1) = 3 \triangleright 1$ . Since  $1 \triangleright 2 \neq 2$  and  $1 \triangleright 3 \neq 3$  we conclude that  $3 \triangleright 1 \notin \{1, 2, 3\}$ . Let  $4 = 3 \triangleright 1$ . Then

$$\mathcal{O}(1, 2) = [4 \ 3 \ 1 \ 2].$$

Therefore  $\varphi_4 = (23)$  and  $\varphi_2 = \varphi_3 = (14)$ . Since  $X$  is indecomposable, this is a contradiction to Lemma 2.23 with  $Y_1 = \{2, 3\}$ ,  $Y_2 = \{1, 4\}$ .

*Step 3.*  $n > 4$ . Let  $y_4, y_5, \dots, y_n \in X$  such that

$$\mathcal{O}(1, 2) = [y_n \ \dots y_5 y_4 \ 3 \ 1 \ 2].$$

On the one hand, by acting with 1 we obtain that

$$\mathcal{O}(1, 3) = [y_n \ \dots y_5 y_4 \ 2 \ 1 \ 3].$$

On the other hand,  $\mathcal{O}(1, 3) = [y_4 y_5 \ \dots y_n \ 2 \ 1 \ 3]$  by Lemma 2.29 and Equation (2.5). This is a contradiction to  $y_4 \neq y_n$ .

**3.2. The case  $k_3 + k_4 + \dots = 3$ .** By Lemma 2.25(3),(4) we may assume without loss of generality that  $\varphi_1 = (234)$ . Let  $n = \#\mathcal{O}(1, 2)$ . By Remark 2.24 we conclude that

$$n = \#\mathcal{O}(1, 3) = \#\mathcal{O}(1, 4).$$

Therefore  $k_n = 3$  and  $k_m = 0$  for all  $m \geq 3$  with  $m \neq n$ . Remark 2.35 implies that  $n \in \{3, 4, 5, 6\}$ . We split the proof in two steps.

*Step 1.*  $n = 3$ . Then  $\mathcal{O}(1, 2) = [3 \ 1 \ 2]$ ,  $\mathcal{O}(1, 3) = [4 \ 1 \ 3]$ , and  $\mathcal{O}(1, 4) = [2 \ 1 \ 4]$ . Since all permutations  $\varphi_i$  with  $i \in X$  have the same cycle structure, we conclude that

$$\varphi_2 = (3 \ 1 \ 4), \quad \varphi_3 = (4 \ 1 \ 2), \quad \varphi_4 = (2 \ 1 \ 3).$$

Since  $X$  is indecomposable, Lemma 2.23 with  $Y_1 = Y_2 = \{1, 2, 3, 4\}$  implies that  $d = 4$ . Then  $X$  is the rack  $\mathcal{T}$ , the rack associated to the vertices of the tetrahedron. The isomorphism  $X \rightarrow \mathcal{T}$  is given by  $i \mapsto \pi_i$ .

*Step 2.*  $n \geq 4$ . Since  $1 \triangleright 2 \neq 2$ , it follows that  $2 \triangleright 1 \neq 1$ , and hence there exist  $i, j \in X$  with  $\varphi_2 = (1 \ i \ j)$ . Since  $n \geq 4$ , we conclude that  $\mathcal{O}(1, 4) = [\dots i \ 2 \ 1 \ 4]$  and  $i \notin \{1, 2, 4\}$ ,  $j \notin \{1, 2, i\}$ . Up to renaming the variables we may assume that  $i \in \{3, 5\}$ .

*Step 2.1.* Assume that  $\varphi_2 = (1 \ 3 \ j)$ . By conjugation with  $\varphi_1$  and by Equation (2.1) we obtain that  $\varphi_3 = (1 \ 4 \ (1 \triangleright j))$ . In the same way, since  $2 \triangleright 1 = 3$ , we conclude that  $\varphi_3 = \varphi_2 \varphi_1 \varphi_2^{-1} = (2 \ j \ (2 \triangleright 4))$ . Comparing the two formulas for  $\varphi_3$  implies that  $\varphi_3 = (1 \ 4 \ 2) = (2 \ 1 \ 4)$ , a contradiction to  $j \neq 1$ .

*Step 2.2.* Assume that  $\varphi_2 = (15j)$ , where  $j \notin \{1, 2, 5\}$ . By conjugation with  $\varphi_1$  we obtain that  $\varphi_3 = (15(1 \triangleright j))$ . Since  $\varphi_3^2 \varphi_2(1) = 1$ , Lemma 2.1 gives that  $\varphi_3^2 \varphi_2 \varphi_1 = \varphi_1 \varphi_3^2 \varphi_2$ . Evaluating this equation at 5 yields that

$$(3.2) \quad \varphi_3^2(j) = \varphi_1 \varphi_3^2(j).$$

Thus  $\varphi_3^2(j) \notin \{2, 3, 4\}$ . Therefore  $1 \triangleright j = j$ , since otherwise  $\varphi_3(j) = j$  which would be a contradiction to Equation (3.2). Conjugation of  $\varphi_2$  by powers of  $\varphi_1$  yields that  $\varphi_2 = \varphi_3 = \varphi_4 = (15j)$  and  $j \notin \{1, 2, 3, 4, 5\}$ . Since  $X$  is indecomposable, this is a contradiction to Lemma 2.23 with  $Y_1 = \{2, 3, 4\}$ ,  $Y_2 = \{1, 5, j\}$ .

**3.3. The case  $k_3 + k_4 + \dots = 4$ .** By Lemma 2.25(3),(4) we know that  $\varphi_1$  has  $d - 4$  fixed points. Therefore, we have to consider two cases:  $\varphi_1 = (23)(45)$  or  $\varphi_1 = (2345)$ .

*Step 1.*  $\varphi_1 = (23)(45)$ .

By Remark 2.24 we may assume that  $\#\mathcal{O}(1, 2) = \#\mathcal{O}(1, 3) = p$  and  $\#\mathcal{O}(1, 4) = \#\mathcal{O}(1, 5) = q$ , where  $3 \leq p \leq q$ . If  $p = q$  then  $k_p = 4$  and then  $p \in \{3, 4\}$  by Remark 2.35. If  $p < q$  then  $k_p = k_q = 2$ . Hence  $p \leq 4$  by Relation (2.7). A closer look at Relation (2.7) gives that one of the following holds.

- $k_3 = 4$  and  $k_n = 0$  for  $n > 3$ .
- $k_4 = 4$  and  $k_n = 0$  for  $n \geq 3$ ,  $n \neq 4$ .
- $k_3 = k_q = 2$ , where  $q \in \{4, 5, 6\}$ , and  $k_n = 0$  for  $n \geq 4$ ,  $n \neq q$ .

We divide the classification of these cases into two steps. In the first step we assume that  $k_3 \geq 2$  and in the second step we consider the remaining case when  $k_4 = 4$ .

*Step 1.1.*  $k_3 \geq 2$ . Then  $\mathcal{O}(1, 2) = [3 \ 1 \ 2]$  and  $\mathcal{O}(1, 3) = [2 \ 1 \ 3]$ , and hence up to renaming we may assume that  $\varphi_2 \in \{(13)(45), (13)(46), (13)(67)\}$ . However, if  $2 \triangleright 6 = 7$  then

$$7 = 1 \triangleright 7 = (2 \triangleright 3) \triangleright 7 \stackrel{(2.1)}{=} 2 \triangleright (3 \triangleright 6) = 2 \triangleright ((1 \triangleright 2) \triangleright 6) \stackrel{(2.1)}{=} 2 \triangleright (1 \triangleright (2 \triangleright 6)) = 6,$$

a contradiction.

Next we show that  $\varphi_2 \neq (13)(45)$ . Indeed, assume that  $2 \triangleright 4 = 5$  and let  $i = 4 \triangleright 1$ . Then  $4 \triangleright i = 1$  since  $X$  is involutive. Moreover,  $\varphi_3 = \varphi_{2 \triangleright 1} = (12)(45)$  by Equation (2.1). First,  $i \neq 1$  by Remark 2.22 since  $1 \triangleright 4 \neq 4$ . Second, Lemma 2.8 with  $(a, b, c) = (1, 4, 1 \triangleright i)$  implies that  $i \notin \{2, 3\}$ . Third,  $i \neq 4$  since  $\varphi_4$  is injective and  $4 \triangleright 4 = 4$ . Finally, Lemma 2.7 with  $(a, b, c, d) = (1, 2, 4, i)$  implies that  $i \notin \{5, 6\}$ , a contradiction.

By the above we conclude that  $\varphi_2 = (13)(46)$ , and hence Equation (2.1) gives that  $\varphi_3 = \varphi_2 \varphi_1 \varphi_2^{-1} = (12)(56)$ .

**Lemma 3.1.** *The orbit  $\mathcal{O}(1, 4)$  has size 3.*

*Proof.* Assume that  $\#\mathcal{O}(1, 4) > 3$ . Then  $4 \triangleright 1 \neq 5$ . Indeed, if  $4 \triangleright 1 = 5$  then  $4 \triangleright 5 = 1$  and hence  $\mathcal{O}(1, 4) = [5 \ 1 \ 4]$ , a contradiction.

Remark 2.22 and (R1) yield that  $4 \triangleright 1 \notin \{1, 4\}$ . Moreover,  $4 \triangleright 1 \neq 3$ . Indeed, otherwise  $4 \triangleright 3 = 1$  since  $X$  is involutive. However,  $3 \triangleright 4 = 4$  and Remark 2.22 imply that  $4 \triangleright 3 = 3$ , a contradiction.

By the above we conclude that  $4 \triangleright 1 \in \{2, 6, 7\}$ . If  $4 \triangleright 1 = 2$  then

$$6 \triangleright 3 = \varphi_2(4 \triangleright 1) = 2, \quad 5 \triangleright 1 = \varphi_1(4 \triangleright 1) = 3.$$

Then Lemma 2.5 with  $Y = \{1, 2, 3\}$  yields a contradiction since  $X$  is indecomposable. Lemma 2.6 with  $(a, x, y, z) = (3, 4, 1, 7)$  implies that  $4 \triangleright 1 \neq 7$ . Finally, if

$4 \triangleright 1 = 6$  then  $4 \triangleright 2 = \varphi_3(4 \triangleright 1) = 5$  and hence

$$\varphi_4 = (16)(25), \quad \varphi_5 = (16)(34), \quad \varphi_6 = (34)(25)$$

by Equation (2.1) using conjugation with  $\varphi_1$  and  $\varphi_2$ , respectively. Then

$$\varphi_4 \varphi_5 \varphi_4^{-1} = (16)(34) \neq \varphi_2,$$

a contradiction to Equation (2.1). Thus  $\#\mathcal{O}(1, 4) = 3$ .  $\square$

Lemma 3.1 gives that  $k_3 = 4$  and  $k_n = 0$  for all  $n > 3$ . Thus  $\#\mathcal{O}(1, i) = 3$  for all  $i \in \{2, 3, 4, 5\}$  and hence

$$\mathcal{O}(1, 2) = [3 \ 1 \ 2], \quad \mathcal{O}(1, 3) = [2 \ 1 \ 3], \quad \mathcal{O}(1, 4) = [5 \ 1 \ 4], \quad \mathcal{O}(1, 5) = [4 \ 1 \ 5].$$

Then  $4 \triangleright 2 = (3 \triangleright 4) \triangleright (3 \triangleright 1) = 3 \triangleright (4 \triangleright 1) = 3 \triangleright 5 = 6$ . We have  $\varphi_4 = (15)(26)$ ,  $\varphi_5 = (14)(36)$  and  $\varphi_6 = (24)(35)$ . Since  $X$  is indecomposable, Lemma 2.23 with  $Y_1 = Y_2 = \{1, 2, \dots, 6\}$  implies that  $d = 6$ . This rack is isomorphic to  $\mathcal{A}$ . The isomorphism  $X \rightarrow \mathcal{A}$  is given by  $i \mapsto \pi_{p(i)}$ , where  $p = (12)(45)$ .

*Step 1.2.*  $k_4 = 4$  and  $k_n = 0$  for all  $n \geq 3$  with  $n \neq 4$ . Then the orbits  $\mathcal{O}(1, 2)$  and  $\mathcal{O}(1, 3)$  have size 4. Since  $X$  is involutive, we conclude from Corollary 2.33 that 1 and  $2 \triangleright 1$  commute, and hence we may assume that  $2 \triangleright 1 = 6$ . Conjugation by  $\varphi_1$  yields that  $3 \triangleright 1 = 6$ , and hence

$$\mathcal{O}(1, 2) = [6 \ 3 \ 1 \ 2], \quad \mathcal{O}(1, 3) = [6 \ 2 \ 1 \ 3].$$

Then  $2 \triangleright \mathcal{O}(1, 2) = [1 \ 2 \triangleright 3 \ 6 \ 2] = [6 \ 2 \ 1 \ 2 \triangleright 3]$ , that is,  $2 \triangleright 3 = 3$ . Up to renaming we obtain that  $\varphi_2 \in \{(16)(45), (16)(47), (16)(78)\}$ . The same arguments applied to  $\mathcal{O}(1, 4)$  and  $\mathcal{O}(1, 5)$ , which also have size 4, give that  $4 \triangleright 1 = 5 \triangleright 1 \in X \setminus \{1, 2, 3, 4, 5\}$  and  $4 \triangleright 5 = 5$ . If  $4 \triangleright 1 = 6$  then Lemma 2.5 with  $Y = \{1, 6\}$  gives a contradiction since  $X$  is indecomposable. Therefore

$$(3.3) \quad 4 \triangleright 1 = 5 \triangleright 1 \in X \setminus \{1, 2, 3, 4, 5, 6\}.$$

*Case 1.* Assume that  $\varphi_2 = (16)(45)$ . Then  $\varphi_3 = \varphi_{1 \triangleright 2} = \varphi_2$  and  $\varphi_6 = \varphi_{2 \triangleright 1} = \varphi_1$  by Equation (2.1). By the above we may assume that  $4 \triangleright 1 = 7$ . Since neither 2 nor 3 commutes with 4, we conclude that  $\varphi_4 = (17)(23)$ . Then  $\varphi_5 = \varphi_{1 \triangleright 4} = \varphi_4$  and  $\varphi_7 = \varphi_{4 \triangleright 1} = \varphi_1$ . Then  $X \triangleright \{4, 5\} \subseteq \{4, 5\}$  which is a contradiction to Lemma 2.5.

*Case 2.* Assume that  $\varphi_2 = (16)(78)$ . Then  $\varphi_3 = \varphi_{1 \triangleright 2} = \varphi_2$  and  $\varphi_6 = \varphi_{2 \triangleright 1} = \varphi_1$ . Since  $2 \triangleright 7 \neq 7$  and  $3 \triangleright 7 \neq 7$ , we conclude that  $\varphi_7 \in \{(23)(ij), (2i)(3j)\}$  for some  $i, j \in X \setminus \{2, 3, 7\}$  with  $i \neq j$ . If  $7 \triangleright 2 = 3$  then  $\varphi_8 = \varphi_{2 \triangleright 7} = (23)(2 \triangleright i \ 2 \triangleright j)$ , and hence  $X \triangleright \{2, 3\} \subseteq \{2, 3\}$  in contradiction to Lemma 2.5. Therefore  $\varphi_7 = (2i)(3j)$ . Applying  $\varphi_1$  we conclude that  $i, j \in \{4, 5\}$ . Let  $k \in \{2, 3\}$  such that  $7 \triangleright k = 4$ . Then  $4 \triangleright 6 = (7 \triangleright k) \triangleright (7 \triangleright 6) = 7 \triangleright (k \triangleright 6) = 7 \triangleright 1 = 1$ , which contradicts to (3.3).

*Case 3.* Assume that  $\varphi_2 = (16)(47)$ . It follows that  $\varphi_3 = \varphi_{1 \triangleright 2} = (16)(57)$  and  $\varphi_6 = \varphi_{2 \triangleright 1} = (23)(57)$ . Moreover,  $\varphi_6 = \varphi_{3 \triangleright 1} = (23)(47)$ , a contradiction.

We conclude that there are no racks satisfying the assumption in Step 1.2. The only solution of Step 1 is the rack  $\mathcal{A}$ .

*Step 2.*  $\varphi_1 = (2345)$ . Let  $m = \#\mathcal{O}(1, 2)$ . Remark 2.24 implies that  $k_m = 4$  and that  $k_n = 0$  for all  $n \geq 3$  with  $n \neq m$ . By Remark 2.35 it follows that  $m \in \{3, 4\}$ .

*Step 2.1.*  $k_3 = 4$  and  $k_n = 0$  for all  $n > 3$ . Then

$$\mathcal{O}(1, 2) = [3 \ 1 \ 2], \quad \mathcal{O}(1, 3) = [4 \ 1 \ 3], \quad \mathcal{O}(1, 4) = [5 \ 1 \ 4], \quad \mathcal{O}(1, 5) = [2 \ 1 \ 5].$$

Therefore  $\varphi_2 = (3 \ 1 \ 5 \ i)$  for some  $i \in X$ , and without loss of generality we may assume that  $i \in \{4, 6\}$ .

*Case 1.* If  $2 \triangleright 5 = 4$  then  $\varphi_3 = \varphi_{1 \triangleright 2} = (4 \ 1 \ 2 \ 5)$  and hence  $\varphi_2 = \varphi_{3 \triangleright 1} = (5 \ 3 \ 1 \ 4)$ , a contradiction.

*Case 2.* If  $2 \triangleright 5 = 6$  then  $\varphi_2 = (1 \ 5 \ 6 \ 3)$ , and by applying  $\varphi_1$  we obtain that  $\varphi_3 = (1 \ 2 \ 6 \ 4)$ ,  $\varphi_4 = (1 \ 3 \ 6 \ 5)$ ,  $\varphi_5 = (1 \ 4 \ 6 \ 2)$ . Moreover,  $\varphi_6 = \varphi_{2 \triangleright 5} = (2 \ 5 \ 4 \ 3)$ . Since  $X$  is indecomposable, Lemma 2.23 with  $Y_1 = Y_2 = \{1, 2, \dots, 6\}$  implies that  $d = 6$ . This rack is  $\mathcal{B}$ .

*Step 2.2.*  $k_4 = 4$  and  $k_n = 0$  for all  $n \geq 3$  with  $n \neq 4$ . Since  $1 \triangleright 2 = 3$ , it follows that  $\mathcal{O}(1, 2) = [i \ 3 \ 1 \ 2]$  for some  $i \in X \setminus \{1, 2, 3\}$ . We may assume that  $i \in \{4, 5, 6\}$ .

*Case 1.*  $3 \triangleright 1 = 4$ . Then  $\mathcal{O}(1, 2) = [1 \ 2 \ 4 \ 3]$ , and by conjugation with  $\varphi_1$  we conclude that

$$\mathcal{O}(1, 3) = [1 \ 3 \ 5 \ 4], \quad \mathcal{O}(1, 4) = [1 \ 4 \ 2 \ 5], \quad \mathcal{O}(1, 5) = [1 \ 5 \ 3 \ 2].$$

Therefore  $\varphi_2 = (5 \ 4 \ 1 \ 3)$ . Conjugation with  $\varphi_1$  yields that  $\varphi_3 = (2 \ 5 \ 1 \ 4)$ ,  $\varphi_4 = (3 \ 2 \ 1 \ 5)$  and  $\varphi_5 = (4 \ 3 \ 1 \ 2)$ . Since  $X$  is indecomposable, Lemma 2.23 with  $Y_1 = Y_2 = \{1, 2, 3, 4, 5\}$  implies that  $d = 5$ . This rack is the affine rack associated with  $(\mathbb{F}_5, 3)$ .

*Case 2.*  $3 \triangleright 1 = 5$ . As in the previous case we obtain that

$$\begin{aligned} \mathcal{O}(1, 2) &= [1 \ 2 \ 5 \ 3], & \mathcal{O}(1, 3) &= [1 \ 3 \ 2 \ 4], \\ \mathcal{O}(1, 4) &= [1 \ 4 \ 3 \ 5], & \mathcal{O}(1, 5) &= [1 \ 5 \ 4 \ 2] \end{aligned}$$

and that

$$\varphi_2 = (5 \ 1 \ 4 \ 3), \quad \varphi_3 = (2 \ 1 \ 5 \ 4), \quad \varphi_4 = (3 \ 1 \ 2 \ 5), \quad \varphi_5 = (4 \ 1 \ 3 \ 2).$$

Since  $X$  is indecomposable, Lemma 2.23 with  $Y_1 = Y_2 = \{1, 2, \dots, 5\}$  implies that  $d = 5$ . This rack is the affine rack associated to  $(\mathbb{F}_5, 2)$ .

*Case 3.*  $3 \triangleright 1 = 6$ . Then  $\mathcal{O}(1, 2) = [1 \ 2 \ 6 \ 3]$ . Conjugation with  $\varphi_1$  gives that  $\mathcal{O}(1, 3) = [1 \ 3 \ 6 \ 4]$ . Hence  $3 \triangleright 1 = 6$  and  $3 \triangleright 6 = 1$ , a contradiction since  $\varphi_3$  is a 4-cycle.

**3.4. The case  $k_3 + k_4 + \dots = 5$ .** By Lemma 2.25(3),(4) we may assume that  $\varphi_1 \in \{(2 \ 3 \ 4 \ 5 \ 6), (2 \ 3)(4 \ 5 \ 6)\}$ .

*Step 1.*  $\varphi_1 = (2 \ 3 \ 4 \ 5 \ 6)$ . Remark 2.24 implies that  $k_m = 5$  for some  $m \geq 3$  and that  $k_n = 0$  for all  $n \geq 3$  with  $n \neq m$ . By Remark 2.35 we obtain that  $m = 3$ . Thus  $\#\mathcal{O}(i, j) = 3$  for all  $i, j \in X$  with  $i \triangleright j \neq j$ . As in Subsection 3.3, Step 2.1. we conclude that  $\varphi_2 = (3 \ 1 \ 6 \ \dots)$ ,  $\varphi_3 = (4 \ 1 \ 2 \ \dots)$ ,  $\varphi_4 = (5 \ 1 \ 3 \ \dots)$ ,  $\varphi_5 = (6 \ 1 \ 4 \ \dots)$  and  $\varphi_6 = (2 \ 1 \ 5 \ \dots)$ . Therefore  $2 \triangleright 6 \in \{4, 5, 7\}$ . Since

$$(3.4) \quad 6 \triangleright (2 \triangleright 6) = (6 \triangleright 2) \triangleright 6 = 1 \triangleright 6 = 2$$

and  $\varphi_6$  is a 5-cycle, it follows that  $2 \triangleright 6 \neq 5$ . If  $2 \triangleright 6 = 7$ , applying  $\varphi_1$  we have that  $3 \triangleright 2 = 4 \triangleright 3 = 5 \triangleright 4 = 6 \triangleright 5 = 7$ , which contradicts (3.4) since  $\varphi_6$  is a 5-cycle. Therefore  $2 \triangleright 6 = 4$  and by applying  $\varphi_1$  we obtain that  $3 \triangleright 2 = 5$ ,  $4 \triangleright 3 = 6$ ,  $5 \triangleright 4 = 2$  and  $6 \triangleright 5 = 3$ . Moreover,  $2 \triangleright 5 \neq 5$  by Remark 2.22 and since  $5 \triangleright 2 \neq 2$ . Hence

$\varphi_2 = (31645)$ ,  $\varphi_3 = (12564)$ ,  $\varphi_4 = (13625)$ ,  $\varphi_5 = (14236)$  and  $\varphi_6 = (15342)$ . However there is no such rack, since for example  $3 \triangleright (6 \triangleright 4) \neq (3 \triangleright 6) \triangleright (3 \triangleright 4)$ .

*Step 2.*  $\varphi_1 = (23)(456)$ . Let  $p = \#\mathcal{O}(1, 2)$  and let  $q = \#\mathcal{O}(1, 4)$ . Since  $1 \triangleright 2 \neq 2$  and  $1 \triangleright 4 \neq 4$ , it follows that  $p, q \geq 3$ . Remark 2.24 implies that  $k_q \geq 3$ . If  $p = q$  then  $k_p = 5$ , and therefore  $p = 3$  by Remark 2.35. If  $p \neq q$  then  $k_p = 2$  and  $k_q = 3$ , since  $k_3 + k_4 + \dots = 5$ . In this case  $p = 4$ ,  $q = 3$  by (2.7). Indeed, if  $p < q$  then  $\frac{p-2}{2p}k_p + \frac{q-2}{2q}k_q \geq \frac{3-2}{6}2 + \frac{4-2}{8}3 = \frac{13}{12} > 1$ , and if  $q < p$  then  $\frac{p-2}{2p}k_p + \frac{q-2}{2q}k_q \geq \frac{4-2}{8}2 + \frac{3-2}{6}3 = 1$ , and equality holds if and only if  $q = 3$ ,  $p = 4$ . This means that

$$(3.5) \quad \mathcal{O}(1, 4) = [5 \ 1 \ 4], \quad \mathcal{O}(1, 5) = [6 \ 1 \ 5], \quad \mathcal{O}(1, 6) = [4 \ 1 \ 6].$$

Hence  $\varphi_4 = (516)(\dots)$ ,  $\varphi_5 = (614)(\dots)$  and  $\varphi_6 = (415)(\dots)$ . Since  $\varphi_1^3 = (23)$ , it follows that  $\varphi_1^3(6) = 6$  and hence  $\varphi_1^3\varphi_6\varphi_1^{-3} = \varphi_6$ . Therefore  $\varphi_6 = (154)(23)$  or  $\varphi_6 = (154)(78)$ .

Assume first that  $\varphi_6 = (154)(78)$ . Then  $6 \triangleright 2 = 2$ , and hence  $2 \triangleright 6 = 6$  by Remark 2.22. By applying  $\varphi_1^2 = (465)$  twice we obtain that  $2 \triangleright 5 = 5$  and  $2 \triangleright 4 = 4$ . Then

$$4 = 2 \triangleright 4 = 2 \triangleright (5 \triangleright 1) = (2 \triangleright 5) \triangleright (2 \triangleright 1) = 5 \triangleright (2 \triangleright 1),$$

and hence  $2 \triangleright 1 = 1$ , which contradicts  $1 \triangleright 2 = 3$  and Remark 2.22.

Assume now that  $\varphi_6 = (154)(23)$ . Then  $2 \triangleright 6 \neq 6$ , and by conjugation with  $\varphi_1^2$  we obtain that  $2 \triangleright 5 \neq 5$ ,  $2 \triangleright 4 \neq 4$ . Thus there exists  $i \in X$  such that  $\varphi_2$  permutes  $\{1, i, 4, 5, 6\}$ . Since  $\varphi_1^2(2) = 2$ , Lemma 2.1 gives that  $\varphi_1^2\varphi_2\varphi_1^{-2} = \varphi_2$ . Therefore  $\varphi_2 \in \{(1i)(456), (1i)(465)\}$ , and we obtain a contradiction to  $\varphi_6^2\varphi_2\varphi_6^{-2} = \varphi_2$ , where the latter holds by Lemma 2.1 and since  $\varphi_6^2(2) = 2$ .

**3.5. The case  $k_3 + k_4 + \dots = 6$ .** By Lemma 2.25(3),4 we obtain that  $\varphi_1 \in \{(234567), (23)(4567), (234)(567), (23)(45)(67)\}$ .

**Lemma 3.2.** *We have  $k_3 = 6$  and  $k_n = 0$  for all  $n > 3$ .*

*Proof.* Let us say that an orbit  $\mathcal{O}(1, i)$  with  $i \in X \setminus \{1\}$  has weight  $\frac{s-2}{2s}$ , where  $s$  is the size of the orbit. Then the left hand side of (2.7) is just the weight sum of the orbits  $\mathcal{O}(1, i)$  of size at least 3, where  $i \in X \setminus \{1\}$ . By assumption there are 6 such orbits, and the smallest weight is  $1/6$  which appears if the orbit size is 3. Hence (2.7) implies that all weights are  $1/6$ , that is, all orbits have size 3. This proves the claim.  $\square$

*Step 1.*  $\varphi_1 = (234567)$ . By Lemma 3.2 and Corollary 2.32 we obtain that  $\varphi_2 = (317\dots)$ ,  $\varphi_3 = (412\dots)$ ,  $\varphi_4 = (513\dots)$ ,  $\varphi_5 = (614\dots)$ ,  $\varphi_6 = (715\dots)$  and  $\varphi_7 = (216\dots)$ . Since

$$7 = 2 \triangleright 1 = 2 \triangleright (3 \triangleright 4) = (2 \triangleright 3) \triangleright (2 \triangleright 4) = 1 \triangleright (2 \triangleright 4),$$

it follows that  $2 \triangleright 4 = 6$ . Moreover,  $2 \triangleright 5 \neq 5$ . Indeed, otherwise

$$7 = 2 \triangleright 1 = 2 \triangleright (4 \triangleright 5) = (2 \triangleright 4) \triangleright (2 \triangleright 5) = 6 \triangleright 5 \neq 7,$$

a contradiction. Therefore  $\varphi_2 \in \{(317465), (317546)\}$ . By conjugation with  $\varphi_1$  one obtains all permutations  $\varphi_i$  with  $i \in \{3, 4, 5, 6, 7\}$ . Since  $X$  is indecomposable, Lemma 2.23 with  $Y_1 = Y_2 = \{1, 2, \dots, 7\}$  implies that  $d = 7$ .



*Case 1.* Assume that  $\varphi_2 = (3\ 1\ 7\ 4\ 6\ 5)$ . Then  $\varphi_3 = (4\ 1\ 2\ 5\ 7\ 6)$ ,  $\varphi_4 = (5\ 1\ 3\ 6\ 2\ 7)$ ,  $\varphi_5 = (6\ 1\ 4\ 7\ 3\ 2)$ ,  $\varphi_6 = (7\ 1\ 5\ 2\ 4\ 3)$  and  $\varphi_7 = (2\ 1\ 6\ 3\ 5\ 4)$ . This rack is the affine rack  $\text{Aff}(7, 5)$ .

*Case 2.* Assume that  $\varphi_2 = (3\ 1\ 7\ 5\ 4\ 6)$ . Then  $\varphi_3 = (4\ 1\ 2\ 6\ 5\ 7)$ ,  $\varphi_4 = (5\ 1\ 3\ 7\ 6\ 2)$ ,  $\varphi_5 = (6\ 1\ 4\ 2\ 7\ 3)$ ,  $\varphi_6 = (7\ 1\ 5\ 3\ 2\ 4)$  and  $\varphi_7 = (2\ 1\ 6\ 4\ 3\ 5)$ . This rack is the affine rack  $\text{Aff}(7, 3)$ .

*Step 2.*  $\varphi_1 = (2\ 3\ 4)(5\ 6\ 7)$ . By Lemma 3.2 and Corollary 2.32 we obtain that  $\varphi_2 = (3\ 1\ 4)(\dots)$ ,  $\varphi_3 = (4\ 1\ 2)(\dots)$ ,  $\varphi_4 = (2\ 1\ 3)(\dots)$ ,  $\varphi_5 = (6\ 1\ 7)(\dots)$ ,  $\varphi_6 = (7\ 1\ 5)(\dots)$  and  $\varphi_7 = (5\ 1\ 6)(\dots)$ . Now we prove two lemmas and prove that they contradict to  $\varphi_1 = (2\ 3\ 4)(5\ 6\ 7)$ . Let  $x, y, z \in X$  such that  $\varphi_2 = (3\ 1\ 4)(xyz)$ .

**Lemma 3.3.** *If  $1 \triangleright y = y$  then  $3 \triangleright x = x$ . Moreover,  $1 \triangleright x \neq x$ .*

*Proof.* From  $2 \triangleright (3 \triangleright x) = (2 \triangleright 3) \triangleright (2 \triangleright x) = 1 \triangleright y = y$  and from (R1) we conclude that  $3 \triangleright x = x$ . If  $1 \triangleright x = x$  then  $x = \varphi_1^2(3 \triangleright x) = \varphi_1^2(3) \triangleright \varphi_1^2(x) = 2 \triangleright x = y$ , a contradiction.  $\square$

**Lemma 3.4.** *We have  $2 \triangleright 5 \neq 6$  and  $2 \triangleright 5 \neq 7$ .*

*Proof.* If  $2 \triangleright 5 = 6$  then  $5 \triangleright 6 = 2$  by Corollary 2.32 and Lemma 3.2. This is a contradiction to  $5 \triangleright 6 = 1$ . Similarly, if  $2 \triangleright 5 = 7$  then  $5 \triangleright 7 = 2$ , a contradiction to  $5 \triangleright 7 = 6$ .  $\square$

Lemma 3.3 implies that at least two of  $x, y, z$  are contained in  $\{5, 6, 7\}$ . By cyclic permutation of  $x, y, z$  and of  $5, 6, 7$  we may assume that  $x, y \in \{5, 6, 7\}$  and that  $x = 5$ . Then Lemma 3.4 gives a contradiction to  $2 \triangleright x = y$ .

We conclude that there are no racks satisfying the properties assumed in Step 2.

*Step 3.*  $\varphi_1 = (2\ 3\ 4\ 5)(6\ 7)$ . Lemma 3.2 and Corollary 2.32 imply that  $\varphi_2 = (3\ 1\ 5)(\dots)$ ,  $\varphi_3 = (4\ 1\ 2)(\dots)$ ,  $\varphi_4 = (5\ 1\ 3)(\dots)$ ,  $\varphi_5 = (2\ 1\ 4)(\dots)$ ,  $\varphi_6 = (1\ 7)(\dots)$  and  $\varphi_7 = (1\ 6)(\dots)$ . Since the role of 6 and 7 is exchangeable, we may assume that  $2 \triangleright 5 \in \{4, 6, 8\}$ . However,  $2 \triangleright 5 \neq 4$ . Indeed, otherwise  $5 \triangleright 4 = 2$  by Corollary 2.32, which is a contradiction to  $\varphi_5 = (2\ 1\ 4)(\dots)$ . Further,  $2 \triangleright 5 \neq 6$ . Indeed, otherwise  $\varphi_2 = (3\ 1\ 5)(\dots)$  and  $5 \triangleright 6 = 2$  by Corollary 2.32. By applying  $\varphi_1$  to the last equation we obtain that  $2 \triangleright 7 = 3$  which is a contradiction to  $2 \triangleright 6 = 3$ . It follows that  $2 \triangleright 5 = 8$ . By applying  $\varphi_1^3$  we conclude that  $5 \triangleright 4 = 8$ .

Since  $8 = 1 \triangleright 8 = (5 \triangleright 2) \triangleright (5 \triangleright 4) = 5 \triangleright (2 \triangleright 4)$  and  $5 \triangleright 4 = 8$ , we obtain from (R1) that  $2 \triangleright 4 = 4$ . Thus  $\varphi_2 \in \{(3\ 1\ 5\ 8)(6\ 7), (3\ 1\ 5\ 8)(6\ 9), (3\ 1\ 5\ 8)(9\ 10)\}$ .

*Step 3.1.*  $\varphi_2 = (3\ 1\ 5\ 8)(6\ 7)$ . Since  $2 \triangleright 6 = 7$ , Corollary 2.32 implies that  $6 \triangleright 7 = 2$ , a contradiction.

*Step 3.2.*  $\varphi_2 = (3\ 1\ 5\ 8)(6\ 9)$ . Then  $6 \triangleright 9 = 2$  by Corollary 2.32. By applying  $\varphi_1^2$  we obtain that  $6 \triangleright 9 = 4$ , a contradiction.

*Step 3.3.*  $\varphi_2 = (3\ 1\ 5\ 8)(9\ 10)$ . Then  $9 \triangleright 10 = 2$  by Corollary 2.32. By applying  $\varphi_1$  we obtain that  $9 \triangleright 10 = 3$ , a contradiction.

It follows that there is no rack  $X$  such that  $k_3 = 6$  and  $\varphi_1 = (2\ 3\ 4\ 5)(6\ 7)$ .

*Step 4.*  $\varphi_1 = (2\ 3)(4\ 5)(6\ 7)$ . Lemma 3.2 implies that

$$\begin{aligned} \mathcal{O}(1, 2) &= [3\ 1\ 2], & \mathcal{O}(1, 3) &= [2\ 1\ 3], & \mathcal{O}(1, 4) &= [5\ 1\ 4], \\ \mathcal{O}(1, 5) &= [4\ 1\ 5], & \mathcal{O}(1, 6) &= [7\ 1\ 6], & \mathcal{O}(1, 7) &= [6\ 1\ 7]. \end{aligned}$$

Hence, since  $4 \triangleright 5 \neq 2$ , it follows from Corollary 2.32 that  $2 \triangleright 4 \neq 5$ . Similarly,  $2 \triangleright 6 \neq 7$ . Further,  $2 \triangleright 8 \neq 9$  since otherwise

$$9 = 1 \triangleright 9 = \varphi_2 \varphi_1(2) \triangleright \varphi_2 \varphi_1(8) = \varphi_2 \varphi_1(2 \triangleright 8) = \varphi_2 \varphi_1(9) = 8,$$

a contradiction. Hence, using our freedom to rename 4, 5, 6, and 7, we may assume that

$$\varphi_2 \in \{(13)(46)(57), (13)(46)(58), (13)(48)(59), (13)(48)(69)\}.$$

*Step 4.1.*  $\varphi_2 = (13)(46)(57)$ . By conjugation with  $\varphi_1$  we obtain that  $\varphi_3 = (12)(57)(46)$ . Since  $\#\mathcal{O}(2,4) = 3$ , it follows from Corollary 2.32 that  $6 \triangleright 2 = 4$ . Similarly,  $\#\mathcal{O}(3,6) = 3$  implies that  $6 \triangleright 4 = 3$ . This is a contradiction since  $\varphi_6^2 = \text{id}$ .

*Step 4.2.*  $\varphi_2 = (13)(46)(58)$ . Conjugation by  $\varphi_1$  yields that  $\varphi_3 = (12)(57)(48)$ , and then  $\varphi_1 = \varphi_{2 \triangleright 3} = (32)(87)(65)$ , a contradiction.

*Step 4.3.*  $\varphi_2 = (13)(48)(59)$ . As in the previous step we obtain that  $\varphi_3 = (12)(58)(49)$  and  $\varphi_1 = \varphi_{2 \triangleright 3} = (32)(94)(85)$ , a contradiction.

*Step 4.4.*  $\varphi_2 = (13)(48)(69)$ . Then conjugation by  $\varphi_1$  yields that  $\varphi_3 = (12)(58)(79)$ . Corollary 2.32 implies that  $\varphi_4 = (15)(28)(\cdot\cdot)$  and  $\varphi_6 = (17)(29)(\cdot\cdot)$ . Since  $1 \triangleright (8 \triangleright 9) = 8 \triangleright 9$  by (R2) and  $8 \triangleright 9 \neq 1$  by Corollary 2.32, it follows that  $8 \triangleright 9 \in \{9, 10\}$ .

First we claim that  $8 \triangleright 9 \neq 9$ . Indeed, otherwise  $2 \triangleright (8 \triangleright 9) = 2 \triangleright 9$ , and hence  $4 \triangleright 6 = 6$  by (R2). However,  $\varphi_6 \neq (54 \triangleright 7)(84 \triangleright 9)(\cdot\cdot) = \varphi_4 \varphi_6 \varphi_4^{-1}$ , a contradiction.

The above arguments yield that  $8 \triangleright 9 = 10$ . By conjugating with  $\varphi_2$  we conclude that  $4 \triangleright 6 = 10$ . It follows from Corollary 2.32 and from (R2) that

$$\begin{aligned} \varphi_1 &= (23)(45)(67), & \varphi_2 &= (13)(48)(69), & \varphi_3 &= (12)(58)(79), \\ \varphi_4 &= (15)(28)(610), & \varphi_5 &= (14)(38)(710), & \varphi_6 &= (17)(29)(410), \\ \varphi_7 &= (16)(39)(510), & \varphi_8 &= (24)(35)(910), & \varphi_9 &= (26)(37)(810), \\ \varphi_{10} &= (46)(57)(89). \end{aligned}$$

This rack is the rack  $\mathcal{C}$ .

#### 4. YETTER-DRINFELD MODULES

We refer to [4] for an introduction to Yetter-Drinfeld modules and Nichols algebras.

Let  $G$  be a group. Let  $g \in G$  and assume that the conjugacy class  $X$  of  $g$  is finite and generates  $G$ . Let  $\mathbb{k}$  be a field and let  $V$  be a Yetter-Drinfeld module over  $\mathbb{k}G$ . Let  $\delta : V \rightarrow \mathbb{k}G \otimes V$  be the left coaction of  $\mathbb{k}G$  on  $V$ . Then  $V = \oplus_{g \in G} V_g$ , where  $V_g = \{v \in V \mid \delta v = g \otimes v\}$ . Moreover,  $hV_g = V_{hgh^{-1}}$  for all  $g, h \in G$ . Yetter-Drinfeld modules can also be studied in terms of racks and two-cocycles, see [2, Thm. 4.14].

For any  $g \in G$  and any representation  $(\rho, W)$  of  $C_G(g)$  let  $M(g, \rho) = \text{Ind}_{C_G(g)}^G \rho$  be the induced  $G$ -module. Then  $M(g, \rho)$  is a Yetter-Drinfeld module over  $G$ . The coaction of  $\mathbb{k}G$  on  $M(g, \rho)$  is given by  $\delta(h \otimes w) = hgh^{-1} \otimes (h \otimes w)$  for all  $h \in G$  and  $w \in W$ .

We write  $\mathfrak{B}(V)$  for the Nichols algebra of  $V$  and  $\mathfrak{B}_n(V)$  for the subspace of homogeneous elements of degree  $n$ , where  $n \in \mathbb{N}_0$ .

For all  $g \in G$  and any linear functional  $f \in V_g^*$  there exists a unique skew-derivation  $\partial_f$  of the Nichols algebra  $\mathfrak{B}(V)$  of  $V$  such that

$$\begin{aligned} \partial_f(v) &= f(v) && \text{for all } v \in V_g, \\ \partial_f(v) &= 0 && \text{for all } v \in V_h \text{ with } h \in G \setminus \{g\}, \\ \partial_f(xy) &= x\partial_f(y) + \partial_f(x)(gy) && \text{for all } x, y \in \mathfrak{B}(V), \end{aligned}$$

see [15, Proof of Lemma 3.5]. If  $\dim V_g = 1$  for some  $g \in G$  then we write  $\partial_v$  for  $\partial_{v^*}$ , where  $v \in V_g$  and  $v^*$  is the dual basis vector of  $v$ .

#### 4.1. Relationship between Nichols algebras over different fields.

**Lemma 4.1.** *Let  $K$  be a field extension of  $\mathbb{k}$  and let  $V_K = K \otimes_{\mathbb{k}} V$ . Then  $V_K$  is a Yetter-Drinfeld module over  $KG$  and any basis of  $\mathfrak{B}(V)$  as a vector space over  $\mathbb{k}$  is a basis of  $\mathfrak{B}(V_K)$  as a vector space over  $K$ . In particular,  $\dim_K \mathfrak{B}(V_K) = \dim_{\mathbb{k}} \mathfrak{B}(V)$ .*

*Proof.* It is clear that any basis of  $\mathfrak{B}(V)$  is spanning  $\mathfrak{B}(V_K)$  as a vector space over  $K$ . The linear independence can be obtained from the description of the Nichols algebra in terms of the quantum symmetrizer.  $\square$

*Remark 4.2.* Assume that  $\text{char } \mathbb{k} = 0$  and that  $V = M(g, \rho)$  for some  $g \in G$  and a one-dimensional representation  $\rho$  of  $C_G(g)$  such that  $\rho(h) \in \{-1, 1\}$  for all  $h \in C_G(g)$ . Let  $d = \dim V$  and let  $p$  be a prime number. Fix  $v \in V_g \setminus \{0\}$ . Then there exist  $g_1, \dots, g_d \in G$  such that  $\{g_1v, \dots, g_dv\}$  is a basis of  $V$ . Let

$$(4.1) \quad \tau_p V = \text{span}_{\mathbb{Z}}\{g_1v, \dots, g_dv\} / \text{span}_{\mathbb{Z}}\{pg_1v, \dots, pg_dv\}.$$

Then  $\tau_p V$  is a Yetter-Drinfeld module over  $\mathbb{F}_p G$ . Up to isomorphism the definition of  $\tau_p V$  does not depend on the choices of  $g_1, \dots, g_d$  and  $v$ .

The following result was proved in [2] for  $\mathbb{k} = \mathbb{C}$ . The proof of the theorem holds without any restriction on  $\mathbb{k}$ .

**Theorem 4.3.** [2, Theorem 6.4] *Assume that  $\mathfrak{B}(V)$  is finite-dimensional. Let  $m \in \mathbb{N}_0$  such that  $\dim \mathfrak{B}_m(V) = 1$  and  $\dim \mathfrak{B}_n(V) = 0$  for all  $n > m$ . Let  $\mathcal{J} \subseteq TV$  be an  $\mathbb{N}_0$ -graded Yetter-Drinfeld submodule over  $\mathbb{k}G$  such that  $\mathcal{J} \cap \mathbb{k} = \mathcal{J} \cap V = 0$ . Assume that  $\mathcal{J}$  is an ideal and a coideal of  $TV$  such that  $\dim T^m V / (\mathcal{J} \cap T^m V) = 1$  and  $\dim T^n V / (\mathcal{J} \cap T^n V) = 0$  for all  $n > m$ . Then  $TV / \mathcal{J} \simeq \mathfrak{B}(V)$ .*

**Theorem 4.4.** *Assume that  $\mathbb{k} = \mathbb{Q}$  and that  $V = M(g, \rho)$  for some  $g \in G$  and a one-dimensional representation  $\rho$  of  $C_G(g)$  such that  $\rho(h) \in \{-1, 1\}$  for all  $h \in C_G(g)$ . Let  $p$  be a prime number. Then the following hold.*

- (1)  $\dim_{\mathbb{F}_p} \mathfrak{B}_n(\tau_p V) \leq \dim_{\mathbb{k}} \mathfrak{B}_n(V)$  for all  $n \in \mathbb{N}_0$ .
- (2) Let  $m \in \mathbb{N}_0$  such that  $\dim_{\mathbb{k}} \mathfrak{B}_m(V) = 1$  and  $\dim_{\mathbb{k}} \mathfrak{B}_n(V) = 0$  for all  $n > m$ . If  $\dim_{\mathbb{F}_p} \mathfrak{B}_m(\tau_p V) \geq 1$  then  $\dim_{\mathbb{F}_p} \mathfrak{B}_n(\tau_p V) = \dim_{\mathbb{k}} \mathfrak{B}_n(V)$  for all  $n \in \mathbb{N}_0$ .

*Proof.* Let  $d = \dim V$  and let  $g_1, \dots, g_d \in G$  such that  $\{g_1v, \dots, g_dv\}$  is a basis of  $V$ . We write  $v_i$  for  $g_i v$  for all  $i \in \{1, \dots, d\}$ . The elements  $v_1, \dots, v_d \in V$  generate an additive subgroup of  $V$  which is denoted by  $W$ . For all  $n \in \mathbb{N}_0$  let  $W^{\otimes_{\mathbb{Z}} n} = W \otimes_{\mathbb{Z}} W \otimes_{\mathbb{Z}} \dots \otimes_{\mathbb{Z}} W$  and let  $f_p : W^{\otimes_{\mathbb{Z}} n} \rightarrow (\tau_p V)^{\otimes_{\mathbb{F}_p} n}$  be the canonical group homomorphism induced by the canonical map  $\mathbb{Z} \rightarrow \mathbb{F}_p$ .

First we prove (1). Let  $n \in \mathbb{N}_0$  and let  $\mathcal{B}$  be a subset of the  $n$ -fold tensor product  $W^{\otimes_{\mathbb{Z}} n}$  consisting of tensor products of generators  $v_i$ ,  $i \in \{1, \dots, d\}$ . Assume that  $f_p(\mathcal{B})$  is linearly independent in  $\mathfrak{B}_n(\tau_p V)$ . It suffices to show that  $\mathcal{B}$  is linearly independent in  $\mathfrak{B}_n(V)$ . We give an indirect proof.

Let  $r \in \mathbb{N}_0$ ,  $b_1, \dots, b_r \in \mathcal{B}$  and  $\lambda_1, \dots, \lambda_r \in \mathbb{Q}$  such that  $\sum_{i=1}^r \lambda_i b_i = 0$  in  $\mathfrak{B}_n(V)$  and that  $\lambda_1 \neq 0$ . Without loss of generality we may assume that  $\lambda_i \in \mathbb{Z}$  for all  $i \in \{1, \dots, r\}$  and that  $\lambda_1 \notin p\mathbb{Z}$ . The assumption on  $\rho$  implies that  $W^{\otimes n}$  is stable under the action of the quantum symmetrizer. Moreover, the map  $f_p$  commutes with the quantum symmetrizer by construction. Then the characterization of Nichols algebras in terms of quantum symmetrizers yields that  $f_p(\mathcal{B})$  is linearly dependent in  $\mathfrak{B}_n(\tau_p V)$ , which proves the claim.

Now we prove (2). For all  $n \in \mathbb{N}_0$  with  $n \geq 2$  let  $U^n \subseteq V^{\otimes n}$  be the kernel of the quantum symmetrizer and let  $U_{\mathbb{Z}}^n = U^n \cap W^{\otimes n}$ . Then  $\oplus_{n \geq 2} U_{\mathbb{Z}}^n / pU_{\mathbb{Z}}^n$  is a Yetter-Drinfeld submodule of the tensor algebra  $T(\tau_p V)$  of  $\tau_p V$  by the assumption on  $\rho$ . Moreover, it is an ideal and a coideal of  $T(\tau_p V)$  since  $U$  is an ideal and a coideal of  $TV$ . Thus  $B = T(\tau_p V) / \oplus_{n \geq 2} U_{\mathbb{Z}}^n / pU_{\mathbb{Z}}^n$  is an  $\mathbb{N}_0$ -graded braided bialgebra in the category of Yetter-Drinfeld modules over  $\mathbb{F}_p G$ . Lemma A.1 yields that

$$(4.2) \quad \mathcal{H}_B(t) = \mathcal{H}_{\mathfrak{B}(V)}(t),$$

where  $\mathcal{H}$  is the Hilbert series. By assumption we know that  $\dim B_m = 1$  and that  $\dim B_n = 0$  for all  $n > m$ . By (1) and the assumption on  $\mathfrak{B}_m(\tau_p V)$  we conclude that  $\dim \mathfrak{B}_m(\tau_p V) = 1$  and  $\dim \mathfrak{B}_n(\tau_p V) = 0$  for all  $n > m$ . By Theorem 4.3 with  $\mathbb{k} = \mathbb{F}_p$  it follows that  $\mathfrak{B}(\tau_p V) \simeq B$ . Thus the claim holds by Equation (4.2).  $\square$

**4.2. Quadratic relations.** Let  $g \in G$  and let  $(\rho, W)$  be a representation of  $C_G(g)$ . We write  $X$  for the conjugacy class of  $g$  in  $G$ . Assume that  $V = M(g, \rho)$ . Then  $V_g \simeq W$  as  $C_G(g)$ -modules. Let  $d$  be the number of elements of  $X$  and let  $e = \dim V_g$ . For any  $H$ -orbit  $\mathcal{O}$  in  $X \times X$ , see Subsection 2.3, let

$$(4.3) \quad V_{\mathcal{O}}^{\otimes 2} = \bigoplus_{(x,y) \in \mathcal{O}} V_x \otimes V_y.$$

Then  $V \otimes V = \bigoplus_{\mathcal{O}} V_{\mathcal{O}}^{\otimes 2}$ , where  $\mathcal{O}$  is running over all  $H$ -orbits in  $X \times X$ .

**Lemma 4.5.** *Let  $r \in V \otimes V$ . For any  $H$ -orbit  $\mathcal{O}$  let  $r_{\mathcal{O}}$  be the projection of  $r$  to  $V_{\mathcal{O}}^{\otimes 2}$ . If  $(1+c)(r) = 0$  then  $(1+c)(r_{\mathcal{O}}) = 0$  for all  $\mathcal{O}$ .*

*Proof.* By construction,  $(1+c)(r_{\mathcal{O}}) \in V_{\mathcal{O}}^{\otimes 2}$  for any  $H$ -orbit  $\mathcal{O}$ . This implies the claim.  $\square$

Assume that  $V$  is finite-dimensional and absolutely irreducible, that is,  $K \otimes_{\mathbb{k}} V$  is an irreducible Yetter-Drinfeld module over  $KG$  for any field extension  $K$  of  $\mathbb{k}$ . In this case the Lemma of Schur implies that any central element in  $C_G(h)$ , where  $h \in X$ , acts on  $V_h$  by a scalar.

*Remark 4.6.* A Yetter-Drinfeld module over  $G$  is absolutely irreducible if and only if it is isomorphic to  $M(h, \sigma)$ , where  $h \in G$  and  $\sigma$  is an absolutely irreducible module of the centralizer  $C_G(h)$ .

**Lemma 4.7.** *Let  $h \in X$  and let  $\mathcal{O} = \mathcal{O}(h, h)$ . Then*

$$\dim(\ker(1+c) \cap V_{\mathcal{O}}^{\otimes 2}) \leq \frac{e(e+1)}{2}.$$

*Proof.* Let  $v_1, \dots, v_e$  be a basis of  $V_h$ . Let  $\lambda \in \mathbb{k}$  such that  $hv = \lambda v$  for all  $v \in V_h$ . Then

$$(1+c)(v_j \otimes v_k) = v_j \otimes v_k + hv_k \otimes v_j = v_j \otimes v_k + \lambda v_k \otimes v_j$$

for all  $j, k \in \{1, \dots, e\}$  with  $j < k$ . Hence  $\text{span}_{\mathbb{k}}\{v_j \otimes v_k \mid j < k\}$  has trivial intersection with  $\ker(1+c)$ . This completes the proof.  $\square$

**Lemma 4.8.** *Let  $h_1, h_2 \in X$  with  $h_1 \neq h_2$  and let  $\mathcal{O} = \mathcal{O}(h_1, h_2)$ . Then*

$$\dim(\ker(1+c) \cap V_{\mathcal{O}}^{\otimes 2}) \leq e^2.$$

*Proof.* Let  $r \in \ker(1+c) \cap V_{\mathcal{O}}^{\otimes 2}$  and for all  $(g_1, g_2) \in \mathcal{O}$  let  $r_{(g_1, g_2)}$  be the projection of  $r$  to  $V_{g_1} \otimes V_{g_2}$ . Since  $h_1 \neq h_2$ , we conclude that  $c(g_1, g_2) \neq (g_1, g_2)$  for all  $(g_1, g_2) \in \mathcal{O}$ . Since  $r \in \ker(1+c)$ , it follows that  $c(r_{(g_1, g_2)}) = -r_{c(g_1, g_2)}$  for all  $(g_1, g_2) \in \mathcal{O}$ . Thus the transitivity of the action of  $H$  on  $\mathcal{O}$  implies that  $r$  is uniquely determined by  $r_{(h_1, h_2)}$ . This completes the proof.  $\square$

Next we demonstrate the calculation of quadratic relations on an example. This result is related to [11, Lemma 2.2]. We prepare the example with the following lemma.

**Lemma 4.9.** *Let  $n \in \mathbb{N}_0$  and let  $x, y \in X$ ,  $v \in V_x$  and  $w \in V_y$ . Then*

$$c^n(v \otimes w) = \begin{cases} (xy)^k x^{-k} v \otimes (xy)^k y^{-k} w & \text{if } n = 2k, k \in \mathbb{N}_0 \\ (xy)^{k+1} y^{-k-1} w \otimes (xy)^k x^{-k} v & \text{if } n = 2k+1, k \in \mathbb{N}_0. \end{cases}$$

*Proof.* By induction on  $n$ .  $\square$

**Example 4.10.** Assume that  $G = G_X$  and that  $\dim V_g = 1$ .

Let  $x \in X$  and let  $\mathcal{O} = \mathcal{O}(x, x)$ . Then  $\dim(V_x \otimes V_x) = 1$ , and  $(1+c)(V_{\mathcal{O}}^{\otimes 2}) = 0$  if and only if  $\rho(g) = -1$ .

Let  $x, y \in X$  with  $x \neq y$ . Let  $\mathcal{O} = \mathcal{O}(x, y)$ . The proof of Lemma 4.8 gives that  $\dim(\ker(1+c) \cap V_{\mathcal{O}}^{\otimes 2}) \leq 1$ . More precisely, let  $r \in V_{\mathcal{O}}^{\otimes 2}$  and for all  $(g_1, g_2) \in \mathcal{O}$  let  $r_{(g_1, g_2)}$  be the projection of  $r$  to  $V_{g_1} \otimes V_{g_2}$ . Then  $r \in \ker(1+c)$  if and only if  $r_{c^n(x, y)} = (-1)^n c^n(r_{(x, y)})$  for all  $n \in \mathbb{N}_0$ . Hence  $\dim(\ker(1+c) \cap V_{\mathcal{O}}^{\otimes 2}) = 1$  if and only if

$$(4.4) \quad \dim(\ker(c^m - (-1)^m) \cap V_x \otimes V_y) = 1,$$

where  $m = \#\mathcal{O}$ . Assume now that  $x = g$  and  $y = hgh^{-1}$ , where  $h \in G_X$  such that  $y = h x h^{-1}$ . Then Lemma 4.9 implies that Equation (4.4) is equivalent to

$$(4.5) \quad \rho(\text{Prod}(hg, h^{-1}g; m) \text{Prod}(h^{-1}g, hg; m)) = (-1)^m \rho(g)^m.$$

Assuming the latter one further obtains that

$$r = \lambda \sum_{n=0}^{m-1} (-1)^n c^n(v \otimes hv),$$

where  $\lambda \in \mathbb{k}$  and  $v \in V_g \setminus \{0\}$ .

Recall the definition of  $k_n$  and  $l_n$ , where  $n \in \mathbb{N}_0$ , from Subsection 2.3.

**Proposition 4.11.** *The dimension of  $\ker(1+c)$  is at most*

$$(4.6) \quad d \frac{e(e+1)}{2} + l_2 e^2 + l_3 e^2 + \dots$$

*Proof.* Follows from Lemmas 4.5, 4.7 and 4.8.  $\square$

*Remark 4.12.* Lemma 2.26 implies that

$$d \frac{e(e+1)}{2} + l_2 e^2 + l_3 e^2 + \dots = e \left( \frac{d(e+1)}{2} + \frac{dk_2}{2} e + \frac{dk_3}{3} e + \dots \right).$$

**Corollary 4.13.** *Assume that  $\dim \ker(1 + c) \geq \dim V(\dim V - 1)/2$ . Then*

$$(4.7) \quad \sum_{n \geq 3} \frac{n-2}{2n} k_n \leq \frac{1}{e}.$$

*Proof.* Recall that  $\dim V = de$ . Since  $\dim \ker(1 + c) \geq de(de - 1)/2$ , Proposition 4.11 and Remark 4.12 imply that

$$\frac{1}{2}de(de - 1) \leq e \left( \frac{d(e+1)}{2} + \frac{dk_2}{2}e + \frac{dk_3}{3}e + \dots \right).$$

Lemma 2.25(4) applied to the left hand side of this inequality yields the claim.  $\square$

For all  $n \in \mathbb{N}_0$  let  $(n)_t = 1 + t + t^2 + \dots + t^{n-1}$ .

**Theorem 4.14.** *Let  $G$  be a group,  $\mathbb{k}$  a field, and  $V$  a Yetter-Drinfeld module over the group algebra  $\mathbb{k}G$ . Assume that  $V$  is finite-dimensional and absolutely irreducible. Then  $V \simeq M(g, \rho)$  for some  $g \in G$  and an absolutely simple representation  $\rho$  of  $C_G(g)$ . Let  $d_V = \dim V$ . The following are equivalent.*

- (1)  $\dim \mathfrak{B}_2(V) \leq \frac{d_V(d_V+1)}{2}$ .
- (2)  $\dim V_g = 1$ , the conjugacy class of  $g$  is isomorphic as a rack to one of the racks listed in Table 2, and the representation of  $C_G(g)$  is given in Table 3, where  $p : G_X \rightarrow G$  is the canonical projection and  $g = px_1$ .
- (3) There exist  $n_1, n_2, \dots, n_{d_V} \in \mathbb{N}_0$  such that the Hilbert series of  $\mathfrak{B}(V)$  factorizes as  $\mathcal{H}_{\mathfrak{B}(V)}(t) = (n_1)_t(n_2)_t \cdots (n_{d_V})_t$ .

*Proof.* First we prove that (1) implies (2). Let  $e = \dim V_g$ . Since

$$\mathfrak{B}_2(V) \simeq V \otimes V / \ker(1 + c),$$

claim (1) implies that  $\dim \ker(1 + c) \geq d_V(d_V - 1)/2$ . By Corollary 4.13 we obtain that

$$\sum_{n \geq 3} \frac{n-2}{2n} k_n \leq \frac{1}{e}.$$

If  $e = 1$  then by Theorem 2.37 the conjugacy class of  $g$  is isomorphic as a rack to one of the racks listed in Table 2. The claim on the representation of  $C_G(g)$  is proved case by case in Section 5.

Assume that  $e \geq 2$ . Then from Theorem 2.37 and the last column of Table 2 we conclude that the conjugacy class of  $g$  is isomorphic as a rack to  $\mathbb{D}_3$  or  $\mathcal{T}$ . Let  $p : G_X \rightarrow G$  be the canonical projection and let  $x \in p^{-1}g$ . Remark 2.21 implies that  $p^{-1}C_G(g) = C_{G_X}(x)$ . The centralizer  $C_{G_X}(x)$  is abelian by Lemmas 5.2 and 5.5, and hence  $C_G(g)$  is abelian. Since  $V$  is absolutely irreducible, Remark 4.6 implies that  $e = \dim V_g = 1$ , a contradiction.

The implication (2)  $\Rightarrow$  (3) is proved case by case in Section 5.

Finally, (3) implies (1) since  $\dim \mathfrak{B}_2(V)$  is the coefficient of  $t^2$  in the Hilbert series  $\mathcal{H}_{\mathfrak{B}(V)}(t)$ .  $\square$

## 5. EXAMPLES

Let  $\mathbb{k}$  be a field and let  $X$  be an indecomposable injective finite rack. Recall that  $G_X$  is the enveloping group of  $X$ . Identify  $X$  with  $\{1, \dots, d\}$ , where  $d = \#X$ , and write  $x_i \in G_X$  for the image of  $i \in X$  in  $G_X$ .

TABLE 3. Centralizers and characters

Rack	Generators of $C_G(px_1)$	Linear character $\rho$ on $C_G(px_1)$
$\mathbb{D}_3$	$px_1$	$\rho(px_1) = -1$
$\mathcal{T}$	$px_1, p(x_4x_2)$	$\rho(px_1) = -1, \rho(p(x_4x_2)) = 1$
$\text{Aff}(5, 2)$	$px_1$	$\rho(px_1) = -1$
$\text{Aff}(5, 3)$	$px_1$	$\rho(px_1) = -1$
$\mathcal{A}$	$px_1, px_4$	$\rho(px_1) = -1, \rho(px_4) = \pm 1$
$\mathcal{B}$	$px_1, px_6$	$\rho(px_1) = \rho(px_6) = -1$
$\text{Aff}(7, 3)$	$px_1$	$\rho(px_1) = -1$
$\text{Aff}(7, 5)$	$px_1$	$\rho(px_1) = -1$
$\mathcal{C}$	$px_1, px_8, px_9$	$\rho(px_1) = -1, \rho(px_8) = \rho(px_9) = \pm 1$

**Lemma 5.1.** *Let  $\rho$  be a linear character of  $C_{G_X}(x_1)$ . Let  $V = M(x_1, \rho)$  and  $d_V = \dim V$ . Assume that  $d_V > 1$ . If  $\dim \mathfrak{B}_2(V) \leq d_V(d_V + 1)/2$  then  $\rho(x_1) = -1$ .*

*Proof.* Assume that  $\rho(x_1) \neq -1$ . Then  $v^2 \neq 0$  in  $\mathfrak{B}(V)$  for all  $v \in V_x \setminus \{0\}$  and all  $x \in X$ . Since  $\dim V_x = 1$  for all  $x \in X$ , we conclude that

$$\dim \mathfrak{B}_2(V) \geq d_V^2 - \#\{\mathcal{O}(x, y) \mid x, y \in X, x \neq y\}$$

by Lemmas 4.5 and 4.8. Since  $d_V > 1$  and  $X$  is indecomposable, it follows that  $\dim \mathfrak{B}_2(V) > d_V(d_V + 1)/2$ , a contradiction.  $\square$

**5.1. The rack  $\mathbb{D}_3$ .** Let  $X = \mathbb{D}_3$ . Then  $\overline{G_X} \simeq \mathbb{S}_3$ . In fact, there is an isomorphism  $\overline{G_X} \rightarrow \mathbb{S}_3$  given by

$$\pi x_1 \mapsto (23), \quad \pi x_2 \mapsto (12), \quad \pi x_3 \mapsto (13).$$

**Lemma 5.2.** *The centralizer of  $x_1$  in  $G_X$  is the cyclic group generated by  $x_1$ .*

*Proof.* Follows from Lemma 2.20(3), since the centralizer of  $\pi x_1$  in  $\mathbb{S}_3$  is the cyclic group generated by  $\pi x_1$ .  $\square$

**Remark 5.3.** Since  $G_{G_X}(x_1)$  is abelian, any absolutely simple representation of  $G_{G_X}(x_1)$  is a linear character. Since  $C_{G_X}(x_1)$  is cyclic, any linear character on  $C_{G_X}(x_1)$  is determined by its action on  $x_1$ .

**Proposition 5.4.** *Let  $\rho$  be an absolutely simple representation of  $C_{G_X}(x_1)$ . Let  $V = M(x_1, \rho)$  and  $d_V = \dim V$ .*

- (1) *The representation  $\rho$  is a linear character on  $C_{G_X}(x_1)$  and hence  $d_V = 3$ . Moreover,  $\dim \mathfrak{B}_2(V) \leq d_V(d_V + 1)/2$  if and only if  $\rho(x_1) = -1$ .*
- (2) *Assume that  $\rho(x_1) = -1$ . Then the following hold.*
  - (a)  $\mathcal{H}_{\mathfrak{B}(V)}(t) = (2)_t^2(3)_t$  and  $\dim \mathfrak{B}(V) = 12$ .
  - (b) *Let  $v_i \in V_{x_i}$  with  $i \in X$  be non-zero elements. Then  $v_1v_2v_1v_3$  is an integral of  $\mathfrak{B}(V)$ .*

*Proof.* The representation  $\rho$  is a linear character on  $C_{G_X}(x_1)$  by Remark 5.3. Further, if  $\dim \mathfrak{B}_2(V) \leq d_V(d_V + 1)/2$  then  $\rho(x_1) = -1$  by Lemma 5.1.

Assume now that  $\rho(x_1) = -1$ . It suffices to prove part (2) of the claim. This follows from [20, Example 6.4].  $\square$



**5.2. The rack  $\mathcal{T}$ .** Let  $X = \mathcal{T}$ . Recall that in  $G_X$  the following relations hold.

$$(5.1) \quad x_1x_2 = x_4x_1 = x_2x_4, \quad x_1x_4 = x_3x_1 = x_4x_3,$$

$$(5.2) \quad x_1x_3 = x_2x_1 = x_3x_2, \quad x_2x_3 = x_4x_2 = x_3x_4.$$

**Lemma 5.5.** *The centralizer of  $x_1$  in  $G_X$  is the abelian group generated by  $x_1$  and  $x_4x_2$ . These elements satisfy the relation  $(x_4x_2)^2 = x_1^4$ .*

*Proof.* First one checks that  $x_4x_2 \in C_{G_X}(x_1)$  and hence  $C = \langle x_4x_2, x_1 \rangle$  is a subgroup of  $C_{G_X}(x_1)$ . Lemmas 2.17 and 2.18 imply that for all  $i \in X$  the elements  $x_i^3 \in G_X$  are central and that  $x_1^3 = x_2^3 = x_3^3 = x_4^3$ . By Equations (5.1) and (5.2) we conclude that

$$G_X/C = \{C, x_2C, x_3C, x_4C\}.$$

Indeed, for example

$$x_2^2C = x_2^2x_1C = x_2x_3x_2C = x_3x_4x_2C = x_3C.$$

Hence  $[G_X : C] \leq 4$ . Since  $\#\mathcal{O}_{x_1} = 4$ , it follows that  $C_{G_X}(x_1) = \langle x_1, x_4x_2 \rangle$ . Moreover,

$$(x_4x_2)^2 = x_4(x_2x_4)x_2 = x_4^2(x_1x_2) = x_4^3x_1$$

and Lemma 2.18 implies that  $x_4^3x_1 = x_1^4$ . This concludes the proof.  $\square$

**Proposition 5.6.** *Let  $\rho$  be an absolutely simple representation of  $C_{G_X}(x_1)$ . Let  $V = M(x_1, \rho)$  and  $d_V = \dim V$ .*

- (1) *The representation  $\rho$  is a linear character on  $C_{G_X}(x_1)$ , hence  $d_V = 4$ . Moreover,  $\dim \mathfrak{B}_2(V) \leq d_V(d_V + 1)/2$  if and only if  $\rho(x_1) = -1$  and  $\rho(x_4x_2) = 1$ .*
- (2) *Assume that  $\text{char } \mathbb{k} \neq 2$ ,  $\rho(x_1) = -1$  and  $\rho(x_4x_2) = 1$ . Then the following hold.*
  - (a)  $\mathcal{H}_{\mathfrak{B}(V)}(t) = (2)_t^2(3)_t(6)_t$  and  $\dim \mathfrak{B}(V) = 72$ .
  - (b) *Let  $v_i \in V_{x_i}$  with  $i \in X$  be non-zero elements. Then  $v_1v_2v_1v_3v_2v_1v_3v_2v_4$  is an integral of  $\mathfrak{B}(V)$ .*
- (3) *Assume that  $\text{char } \mathbb{k} = 2$ ,  $\rho(x_1) = -1$  and  $\rho(x_4x_2) = 1$ . Then the following hold.*
  - (a)  $\mathcal{H}_{\mathfrak{B}(V)}(t) = (2)_t^2(3)_t^2$  and  $\dim \mathfrak{B}(V) = 36$ .
  - (b) *Let  $v_i \in V_{x_i}$  with  $i \in X$  be non-zero elements. Then  $v_1v_2v_1v_3v_2v_4$  is an integral of  $\mathfrak{B}(V)$ .*

*Proof.* The representation  $\rho$  is a linear character on  $C_{G_X}(x_1)$ , since  $C_{G_X}(x_1)$  is abelian. Further, if  $\dim \mathfrak{B}_2(V) \leq d_V(d_V + 1)/2$  then  $\rho(x_1) = -1$  by Lemma 5.1. We prove that if  $\dim \mathfrak{B}_2(V) \leq d_V(d_V + 1)/2$  then  $\rho(x_4x_2) = 1$ . Let  $g = x_1$  and  $h = x_2$ . Then  $hgh^{-1} = x_4$ . Since  $\#\mathcal{O}(x_1, x_4) = 3$ , Example 4.10 implies that  $\dim(\ker(1 + c) \cap V_{\mathcal{O}(x_1, x_4)}^{\otimes 2}) = 1$  if and only if

$$\rho((x_2x_1x_2^{-1}x_1x_2x_1)(x_2^{-1}x_1x_2x_1x_2^{-1}x_1)) = -\rho(x_1)^3.$$

By Equations (5.1)–(5.2) this is equivalent to  $\rho(x_4x_2)\rho(x_1) = -1$ . The group  $G_X$  acts transitively on the set of orbits  $\mathcal{O}(x, y)$  with  $x \neq y$  by diagonal action. Hence  $\dim(\ker(1 + c) \cap V_{\mathcal{O}(x, y)}^{\otimes 2}) = 1$  for  $x \neq y$  if and only if  $\rho(x_4x_2)\rho(x_1) = -1$ . The inequality  $\dim \mathfrak{B}_2(V) \leq d_V(d_V + 1)/2$  is equivalent to  $\dim \ker(1 + c) \geq 6$ . Since there are four orbits  $\mathcal{O}(x, y)$  with  $x = y$  and four orbits with  $x \neq y$ , the inequality  $\dim \mathfrak{B}_2(V) \leq d_V(d_V + 1)/2$  implies that  $\rho(x_1) = -1$  and  $\rho(x_4x_2) = 1$ . The remaining implication in part (1) follows from (2) and (3).

Now we prove (2). For  $\mathbb{k} = \mathbb{C}$  the result is known, see [2, Theorem 6.15]. For other fields  $\mathbb{k}$  of characteristic zero the result follows from Lemma 4.1. Assume now that  $\text{char } \mathbb{k} > 2$ . By the proof of [2, Theorem 6.15] the monomial  $v_1 v_2 v_1 v_3 v_2 v_1 v_3 v_2 v_4$  is non-zero in  $\mathfrak{B}(V)$ . Therefore the claim in (2) holds by Theorem 4.4 for  $\mathbb{k} = \mathbb{F}_p$  with  $p > 2$  and by Lemma 4.1 for arbitrary fields  $\mathbb{k}$  of characteristic  $p > 2$ .

The claims in (3) follow from Proposition 5.7.  $\square$

**Proposition 5.7.** *Assume that  $\text{char } \mathbb{k} = 2$ .*

(1) *Let  $B$  be the algebra given by generators  $a, b, c, d$  and defining relations*

$$(5.3) \quad a^2 = b^2 = c^2 = d^2 = 0,$$

$$(5.4) \quad ba + db + ad = ca + bc + ab = da + cd + ac = cb + dc + bd = 0,$$

$$(5.5) \quad cad + bac + dab = 0.$$

*Then a basis of  $B$  is given by*

$$\begin{aligned} &1, a, b, c, d, ab, ac, ad, ba, bc, bd, cb, cd, \\ &aba, abc, abd, acb, acd, bac, bad, bcb, bcd, cbd, \\ &abac, abad, abcb, abcd, acbd, bacb, bacd, bcbd, \\ &abac, baba, cdab, cbdb, acbd, abacbd. \end{aligned}$$

(2) *Let  $\rho$  be an absolutely simple representation of  $C_{G_X}(x_1)$  such that  $\rho(x_1) = -1$  and  $\rho(x_4 x_2) = 1$ . Let  $V = M(x_1, \rho)$  and let  $v \in V_{x_1} \setminus \{0\}$ . Define*

$$v_1 = v, \quad v_2 = x_3 v, \quad v_3 = x_4 v, \quad v_4 = x_2 v.$$

*Then the linear map  $V \rightarrow B$  given by  $(v_1, v_2, v_3, v_4) \mapsto (a, b, c, d)$  extends uniquely to an algebra isomorphism  $\mathfrak{B}(V) \rightarrow B$ .*

*Proof.* Part (1) can be obtained using the diamond lemma [6] or by calculating a non-commutative Gröbner basis [8, 1]. To prove part (2) it is sufficient to see that  $v_1 v_2 v_1 v_3 v_2 v_4$  does not vanish in  $\mathfrak{B}(V)$ . For this purpose one can show that

$$\partial_{v_2} \partial_{v_1} \partial_{v_4} \partial_{v_1} \partial_{v_2} \partial_{v_3} (v_1 v_2 v_1 v_3 v_2 v_4) = 1.$$

This completes the proof.  $\square$

**5.3. The rack  $\mathcal{A}$ .** Let  $X = \mathcal{A}$ . Recall that in  $G_X$  the following relations hold.

$$(5.6) \quad x_1 x_2 = x_3 x_1 = x_2 x_3, \quad x_1 x_3 = x_2 x_1 = x_3 x_2, \quad x_1 x_4 = x_4 x_1,$$

$$(5.7) \quad x_1 x_5 = x_6 x_1 = x_5 x_6, \quad x_1 x_6 = x_5 x_1 = x_6 x_5, \quad x_2 x_6 = x_6 x_2,$$

$$(5.8) \quad x_2 x_4 = x_5 x_2 = x_4 x_5, \quad x_2 x_5 = x_4 x_2 = x_5 x_4, \quad x_3 x_5 = x_5 x_3,$$

$$(5.9) \quad x_3 x_4 = x_6 x_3 = x_4 x_6, \quad x_3 x_6 = x_4 x_3 = x_6 x_4.$$

**Lemma 5.8.** *The centralizer of  $x_1$  in  $G_X$  is the abelian group generated by  $x_1$  and  $x_4$ . These generators satisfy  $x_1^2 = x_4^2$ .*

*Proof.* By (5.6) we obtain that  $\langle x_1, x_4 \rangle$  is an abelian subgroup of  $C_{G_X}(x_1)$ . Equations (5.6)–(5.9) imply that  $[G_X : \langle x_1, x_4 \rangle] \leq 6$ . Indeed, let  $C = \langle x_1, x_4 \rangle$ . Then  $x_2 x_6 x_1 = x_3 x_5 x_4$ . This and similar calculations yield that

$$G_X / C = \{C, x_3 C, x_2 C, x_5 x_3 C, x_6 C, x_5 C\}.$$

Since  $\#\mathcal{O}_{x_1} = 6$ , it follows that  $C_{G_X}(x_1) = \langle x_1, x_4 \rangle$ . Equation  $x_1^2 = x_4^2$  is obtained from Lemma 2.18.  $\square$

**Proposition 5.9.** *Let  $\rho$  be an absolutely simple representation of  $C_{G_X}(x_1)$ . Let  $V = M(x_1, \rho)$  and  $d_V = \dim V$ .*

- (1) *The representation  $\rho$  is a linear character on  $C_{G_X}(x_1)$ , hence  $d_V = 6$ . Moreover,  $\dim \mathfrak{B}_2(V) \leq d_V(d_V + 1)/2$  if and only if  $\rho(x_1) = -1$ . In this case  $\rho(x_4) \in \{-1, 1\}$ .*
- (2) *Assume that  $\rho(x_1) = -1$ . Then the following hold.*
  - (a)  $\mathcal{H}_{\mathfrak{B}(V)}(t) = (2)_t^2(3)_t^2(4)_t^2$  and  $\dim \mathfrak{B}(V) = 576$ .
  - (b) *Let  $v_i \in V_{x_i}$  with  $i \in X$  be non-zero elements. Then the monomial  $v_1v_2v_1v_3v_4v_2v_1v_3v_4v_5v_1v_6$  is an integral of  $\mathfrak{B}(V)$ .*

*Proof.* We first prove (1). Since  $C_{G_X}(x_1)$  is abelian by Lemma 5.8, we conclude that  $\rho$  is a linear character. Lemma 5.1 implies that  $\rho(x_1) = -1$  and  $\rho(x_4) \in \{-1, 1\}$ . The diagonal action of  $G_X$  on the set of  $H$ -orbits of size 1, 2 and 3, respectively, is transitive. Hence there is a quadratic relation of  $\mathfrak{B}(V)$  corresponding to an  $H$ -orbit of a given size if and only if there is a quadratic relation of  $\mathfrak{B}(V)$  for each  $H$ -orbit of this size. By Example 4.10 the latter holds for all  $H$ -orbits. The cases  $\rho(x_4) = -1$  and  $\rho(x_4) = 1$ , respectively, were discussed in [20, Example 6.4] and in [10, Definition 2.1], respectively. In these papers also  $\mathcal{H}_{\mathfrak{B}(V)}(t)$  was calculated. In both cases one can check that

$$\partial_{v_4}\partial_{v_2}\partial_{v_4}\partial_{v_1}\partial_{v_2}\partial_{v_4}\partial_{v_3}\partial_{v_4}\partial_{v_2}\partial_{v_5}\partial_{v_6}\partial_{v_5}(v_1v_2v_1v_3v_4v_2v_1v_3v_4v_5v_1v_6) = -1.$$

This completes the proof.  $\square$

**5.4. The rack  $\mathcal{B}$ .** Let  $X = \mathcal{B}$ . Then

$$(5.10) \quad x_1^4 = x_2^4 = x_3^4 = x_4^4 = x_5^4 = x_6^4,$$

$$(5.11) \quad x_3x_5 = x_2x_4 = x_1x_6$$

in  $G_X$ .

**Lemma 5.10.** *The centralizer of  $x_1$  in  $G_X$  is the abelian subgroup generated by  $x_1$  and  $x_6$ . These elements satisfy  $x_1^4 = x_6^4$ .*

*Proof.* The proof is similar to the proof of Lemma 5.8.  $\square$

**Proposition 5.11.** *Let  $\rho$  be an absolutely simple representation of  $C_{G_X}(x_1)$ . Let  $V = M(x_1, \rho)$  and  $d_V = \dim V$ .*

- (1) *The representation  $\rho$  is a linear character on  $C_{G_X}(x_1)$ , hence  $d_V = 6$ . Moreover,  $\dim \mathfrak{B}_2(V) \leq d_V(d_V + 1)/2$  if and only if  $\rho(x_1) = \rho(x_6) = -1$ .*
- (2) *Assume that  $\rho(x_1) = -1$  and  $\rho(x_6) = -1$ . Then the following hold.*
  - (a)  $\mathcal{H}_{\mathfrak{B}(V)}(t) = (2)_t^2(3)_t^2(4)_t^2$  and  $\dim \mathfrak{B}(V) = 576$ .
  - (b) *Let  $v_i \in V_{x_i}$  with  $i \in X$  be non-zero elements. Then the monomial  $v_1v_2v_1v_3v_2v_1v_4v_3v_2v_5v_4v_6$  is an integral of  $\mathfrak{B}(V)$ .*

*Proof.* Analogous to the proof of Proposition 5.9 for  $\mathbb{k} = \mathbb{C}$ . The Nichols algebra in part (2) was studied in [2, Theorem 6.12]. The existence of an integral of degree 12 follows from the formula

$$\partial_{v_2}\partial_{v_1}\partial_{v_4}\partial_{v_3}\partial_{v_4}\partial_{v_6}\partial_{v_2}\partial_{v_6}\partial_{v_4}\partial_{v_3}\partial_{v_4}\partial_{v_5}(v_1v_2v_1v_3v_2v_1v_4v_3v_2v_5v_4v_6) = -1.$$

For other fields see the proof of Proposition 5.6.  $\square$

5.5. **The rack  $\mathcal{C}$ .** Let  $X = \mathcal{C}$ .

**Lemma 5.12.** *The centralizer of  $x_1$  in  $G_X$  is the non-abelian group  $\langle x_1 \rangle \times \langle x_8, x_9 \rangle$ . These generators satisfy  $x_1^2 = x_8^2 = x_9^2$  and  $x_8 x_9 x_8 = x_9 x_8 x_9$ .*

*Proof.* The proof is similar to the proof of Lemma 5.8.  $\square$

**Proposition 5.13.** *Let  $\rho$  be an absolutely simple representation of  $C_{G_X}(x_1)$ . Let  $V = M(x_1, \rho)$  and  $d_V = \dim V$ .*

- (1) *We have  $\dim \mathfrak{B}_2(V) \leq d_V(d_V + 1)/2$  if and only if  $\rho$  is a linear character such that  $\rho(x_1) = -1$  and  $\rho(x_8) = \rho(x_9) = \pm 1$ .*
- (2) *Assume that  $\rho$  is a linear character such that  $\rho(x_1) = -1$  and  $\rho(x_8) = \rho(x_9) = \pm 1$ . Then the following hold.*
  - (a)  $\mathcal{H}_{\mathfrak{B}(V)}(t) = (4)_t^4 (5)_t^2 (6)_t^4$  and  $\dim \mathfrak{B}(V) = 8294400$ .
  - (b) *Let  $v_i \in V_{x_i}$  with  $i \in X$  be non-zero elements. Then the monomial*

$$(5.12) \quad \begin{aligned} & v_1 v_2 v_1 v_3 v_4 v_1 v_2 v_1 v_4 v_5 v_3 v_6 v_1 v_2 v_1 v_4 v_1 v_2 v_1 v_4 \times \\ & v_6 v_1 v_2 v_1 v_5 v_3 v_6 v_2 v_4 v_2 v_6 v_7 v_3 v_5 v_3 v_7 v_8 v_9 v_8 v_{10} \end{aligned}$$

*is an integral of  $\mathfrak{B}(V)$ .*

*Proof.* Assume that  $\dim \mathfrak{B}_2(V) \leq d_V(d_V + 1)/2$ . Then  $\rho$  is a linear character by Theorem 4.14. Lemma 5.1 yields that  $\rho(x_1) = -1$ . Equations  $\rho(x_8) = \rho(x_9) = \pm 1$  follow from Lemma 5.12. The remaining claim in (1) follows from part (2).

The statement (2)(a) was first given in [10] in the case that  $\rho(x_8) = 1$  and in [14] in the case that  $\rho(x_8) = -1$ . For a proof for  $\mathbb{k} = \mathbb{C}$  see for example [11, Theorem 2.4]. For other fields proceed as in the proof of Proposition 5.6. The evaluation of the product

$$\begin{aligned} & \partial_{v_4} \partial_{v_1} \partial_{v_3} \partial_{v_5} \partial_{v_4} \partial_{v_2} \partial_{v_5} \partial_{v_4} \partial_{v_6} \partial_{v_7} \partial_{v_3} \partial_{v_9} \partial_{v_6} \partial_{v_{10}} \partial_{v_6} \partial_{v_5} \partial_{v_{10}} \partial_{v_6} \partial_{v_9} \partial_{v_6} \times \\ & \partial_{v_7} \partial_{v_5} \partial_{v_6} \partial_{v_9} \partial_{v_8} \partial_{v_{10}} \partial_{v_7} \partial_{v_6} \partial_{v_5} \partial_{v_3} \partial_{v_5} \partial_{v_7} \partial_{v_9} \partial_{v_8} \partial_{v_{10}} \partial_{v_7} \partial_{v_{10}} \partial_{v_8} \partial_{v_{10}} \partial_{v_9} \end{aligned}$$

of derivations at the monomial given in (5.12) gives  $\rho(x_8)$ . Hence the monomial in (5.12) is an integral.  $\square$

5.6. **Affine Racks.** Let  $X$  be one of the affine racks listed in Table 2.

**Lemma 5.14.** *The centralizer of  $x_1$  in  $G_X$  is the cyclic group generated by  $x_1$ .*

*Proof.* Assume that  $X = \text{Aff}(5, 2)$ . Then  $\overline{G_X}$  is isomorphic to the affine group  $C_5 \rtimes C_4$ . The centralizer in  $\overline{G_X}$  of  $\pi x_1$  in the cyclic subgroup generated by  $\pi x_1$ . Then the claim follows from Lemma 2.20. The proof for the other affine racks is similar.  $\square$

**Proposition 5.15.** *Let  $\rho$  be an absolutely simple representation of  $C_{G_X}(x_1)$ . Let  $V = M(x_1, \rho)$  and  $d_V = \dim V$ .*

- (1) *The representation  $\rho$  is a linear character on  $C_{G_X}(x_1)$  and hence  $d_V = \#X$ . Moreover,  $\dim \mathfrak{B}_2(V) \leq d_V(d_V + 1)/2$  if and only if  $\rho(x_1) = -1$ .*
- (2) *Assume that  $X = \text{Aff}(5, 2)$  or  $X = \text{Aff}(5, 3)$  and that  $\rho(x_1) = -1$ . Then the following hold.*
  - (a)  $\mathcal{H}_{\mathfrak{B}(V)}(t) = (4)_t^4 (5)_t$  and  $\dim \mathfrak{B}(V) = 1280$ .
  - (b) *Let  $v_i \in V_{x_i}$  with  $i \in X$  be non-zero elements. Then*

$$v_1 v_2 v_1 v_2 v_3 v_1 v_2 v_1 v_3 v_1 v_4 v_1 v_4 v_2 v_3 v_5$$

is an integral of  $\mathfrak{B}(V)$  for  $X = \text{Aff}(5, 2)$  and

$$v_1 v_2 v_4 v_3 v_2 v_4 v_5 v_2 v_1 v_3 v_2 v_4 v_3 v_1 v_2 v_4$$

is an integral of  $\mathfrak{B}(V)$  for  $X = \text{Aff}(5, 3)$ .

- (3) Assume that  $X = \text{Aff}(7, 3)$  or  $X = \text{Aff}(7, 5)$  and that  $\rho(x_1) = -1$ . Then the following hold.

- (a)  $\mathcal{H}_{\mathfrak{B}(V)}(t) = (6)_t^6(7)_t$  and  $\dim \mathfrak{B}(V) = 326592$ .  
(b) Let  $v_i \in V_{x_i}$  with  $i \in X$  be non-zero elements. Then

$$(5.13) \quad \begin{aligned} &v_1 v_2 v_1 v_3 v_1 v_2 v_1 v_3 v_1 v_2 v_1 v_3 v_4 v_2 v_1 v_4 v_2 v_3 \times \\ &v_4 v_2 v_1 v_5 v_1 v_3 v_1 v_2 v_1 v_3 v_4 v_2 v_3 v_5 v_1 v_6 v_4 v_7 \end{aligned}$$

is an integral of  $\mathfrak{B}(V)$  for  $X = \text{Aff}(7, 3)$  and

$$(5.14) \quad \begin{aligned} &v_6 v_7 v_6 v_5 v_6 v_7 v_5 v_6 v_5 v_7 v_6 v_5 v_4 v_5 v_6 v_4 v_5 v_7 \times \\ &v_6 v_5 v_7 v_3 v_7 v_6 v_2 v_3 v_4 v_2 v_4 v_3 v_5 v_4 v_3 v_2 v_1 v_2 \end{aligned}$$

is an integral of  $\mathfrak{B}(V)$  for  $X = \text{Aff}(7, 5)$ .

*Proof.* Assume that  $\dim \mathfrak{B}_2(V) \leq d_V(d_V + 1)/2$ . Since  $C_{G_X}(x_1)$  is abelian, the representation  $\rho$  is a linear character. Lemma 5.1 yields that  $\rho(x_1) = -1$ . The remaining claim in (1) follows from parts (2) and (3).

The statement (2) was proved in [2, Theorem 6.16] in the case that  $X = \text{Aff}(5, 2)$  and  $\mathbb{k} = \mathbb{C}$ . In the proof of [2, Theorem 6.16] it was shown that the evaluation of the product

$$\partial_{v_3} \partial_{v_1} \partial_{v_3} \partial_{v_1} \partial_{v_2} \partial_{v_1} \partial_{v_2} \partial_{v_3} \partial_{v_4} \partial_{v_3} \partial_{v_5} \partial_{v_3} \partial_{v_4} \partial_{v_5} \partial_{v_4} \partial_{v_5}$$

of derivations at  $v_1 v_2 v_1 v_2 v_3 v_1 v_2 v_1 v_3 v_1 v_4 v_1 v_4 v_2 v_3 v_5$  gives 1. Thus for fields  $\mathbb{k} \neq \mathbb{C}$  the claim can be proved as in the proof of Proposition 5.6. The case  $X = \text{Aff}(5, 3)$  is similar. The evaluation of the product

$$\partial_{v_2} \partial_{v_1} \partial_{v_2} \partial_{v_1} \partial_{v_3} \partial_{v_1} \partial_{v_4} \partial_{v_3} \partial_{v_5} \partial_{v_3} \partial_{v_5} \partial_{v_4} \partial_{v_3} \partial_{v_5} \partial_{v_3} \partial_{v_5}$$

of derivations at  $v_1 v_2 v_4 v_3 v_2 v_4 v_5 v_2 v_1 v_3 v_2 v_4 v_3 v_1 v_2 v_4$  gives 1.

The statement (3) was proved in [14] in the case that  $\mathbb{k} = \mathbb{C}$ . For other fields proceed as in the proof of Proposition 5.6. For  $X = \text{Aff}(7, 3)$  the evaluation of the product

$$(5.15) \quad \begin{aligned} &\partial_{v_2} \partial_{v_1} \partial_{v_2} \partial_{v_3} \partial_{v_4} \partial_{v_5} \partial_{v_3} \partial_{v_4} \partial_{v_2} \partial_{v_4} \partial_{v_3} \partial_{v_2} \partial_{v_6} \partial_{v_7} \partial_{v_3} \partial_{v_7} \partial_{v_5} \partial_{v_6} \times \\ &\partial_{v_7} \partial_{v_5} \partial_{v_4} \partial_{v_6} \partial_{v_5} \partial_{v_4} \partial_{v_5} \partial_{v_6} \partial_{v_7} \partial_{v_5} \partial_{v_6} \partial_{v_5} \partial_{v_7} \partial_{v_6} \partial_{v_5} \partial_{v_6} \partial_{v_7} \partial_{v_6} \end{aligned}$$

of derivations at the monomial given in (5.13) gives 1.

For  $X = \text{Aff}(7, 5)$  the evaluation of the product

$$\begin{aligned} &\partial_{v_6} \partial_{v_2} \partial_{v_7} \partial_{v_1} \partial_{v_2} \partial_{v_1} \partial_{v_3} \partial_{v_6} \partial_{v_5} \partial_{v_4} \partial_{v_1} \partial_{v_2} \partial_{v_1} \partial_{v_3} \partial_{v_1} \partial_{v_5} \partial_{v_1} \partial_{v_2} \times \\ &\partial_{v_4} \partial_{v_2} \partial_{v_6} \partial_{v_1} \partial_{v_3} \partial_{v_4} \partial_{v_3} \partial_{v_5} \partial_{v_7} \partial_{v_4} \partial_{v_3} \partial_{v_1} \partial_{v_4} \partial_{v_1} \partial_{v_3} \partial_{v_1} \partial_{v_2} \partial_{v_1} \end{aligned}$$

of derivations at the monomial given in (5.14) gives  $-1$ .  $\square$

#### APPENDIX A. AN APPLICATION OF THE ELEMENTARY DIVISORS THEOREM

The following lemma, which is an application of the elementary divisors theorem, is needed for the proof of Theorem 4.4.

**Lemma A.1.** *Let  $V$  be a finite-dimensional vector space over  $\mathbb{Q}$  and let  $U \subseteq V$  be a subspace. Let  $W$  be the free  $\mathbb{Z}$ -module generated by a basis of  $V$  and let  $U_{\mathbb{Z}} = U \cap W$ . Then for all primes  $p$  the quotient  $U_{\mathbb{Z}}/pU_{\mathbb{Z}}$  is a vector space over  $\mathbb{F}_p$  of dimension  $\dim U$ .*

*Proof.* Let  $d = \dim V$ . By the elementary divisors theorem, see [19, Ch. III, Theorem 7.8], there exist a basis  $\{e_1, \dots, e_d\}$  of  $W$ , an integer  $m \in \mathbb{N}_0$  and integers  $a_1, \dots, a_m > 0$  such that  $\{a_1 e_1, \dots, a_m e_m\}$  is a basis of  $U_{\mathbb{Z}}$ . Since  $U$  is a vector space, it follows that  $a_i = 1$  for all  $i \in \{1, \dots, m\}$ . We conclude that  $\{e_1, \dots, e_m\}$  is a basis of  $U$  by definition of  $U_{\mathbb{Z}}$ . Thus  $\dim(U_{\mathbb{Z}}/pU_{\mathbb{Z}}) = \dim U = m$ .  $\square$

*Acknowledgement.* I.H. was supported by the German Research Foundation via a Heisenberg fellowship. M.G. and L.V. was supported by CONICET. The third author thanks DAAD and Philipps-Universität Marburg for the support of his visit in Marburg from December 2009 to March 2010.

## REFERENCES

- [1] The GAP Group, 2006. GAP – Groups, Algorithms, and Programming, Version 4.4.12. Available at <http://www.gap-system.org>.
- [2] N. Andruskiewitsch and M. Graña. From racks to pointed Hopf algebras. *Adv. Math.*, 178(2):177–243, 2003.
- [3] N. Andruskiewitsch and H.-J. Schneider. Lifting of quantum linear spaces and pointed Hopf algebras of order  $p^3$ . *J. Algebra*, 209(2):658–691, 1998.
- [4] N. Andruskiewitsch and H.-J. Schneider. Pointed Hopf algebras. In *New directions in Hopf algebras*, volume 43 of *Math. Sci. Res. Inst. Publ.*, pages 1–68. Cambridge Univ. Press, Cambridge, 2002.
- [5] N. Andruskiewitsch and H.-J. Schneider. On the classification of finite-dimensional pointed Hopf algebras. *Ann. Math.*, 171(1):375–417, 2010.
- [6] G. M. Bergman. The diamond lemma for ring theory. *Adv. in Math.*, 29(2):178–218, 1978.
- [7] J. S. Carter, D. Jelsovsky, S. Kamada, L. Langford, and M. Saito. Quandle cohomology and state-sum invariants of knotted curves and surfaces. *Trans. Amer. Math. Soc.*, 355(10):3947–3989 (electronic), 2003.
- [8] A. Cohen and J. Knopper. GBNP, A GAP Package for Gröbner bases of noncommutative polynomials. Available at <http://dam02.win.tue.nl/products/gbnp/>.
- [9] V. G. Drinfel'd. Quantum groups. In *Proceedings of the International Congress of Mathematicians, Vol. 1, 2 (Berkeley, Calif., 1986)*, pages 798–820, Providence, RI, 1987. Amer. Math. Soc.
- [10] S. Fomin and A. N. Kirillov. Quadratic algebras, Dunkl elements, and Schubert calculus. In *Advances in geometry*, volume 172 of *Progr. Math.*, pages 147–182. Birkhäuser Boston, Boston, MA, 1999.
- [11] G. García and A. García Iglesias. Finite dimensional pointed Hopf algebras over  $\mathbb{S}_4$ , 2009. Israel Journal of Mathematics, to appear.
- [12] M. Geck and G. Pfeiffer. *Characters of finite Coxeter groups and Iwahori-Hecke algebras*, volume 21 of *London Mathematical Society Monographs. New Series*. The Clarendon Press Oxford University Press, New York, 2000.
- [13] M. Graña and L. Vendramin. RIG, A GAP package for racks and Nichols Algebras. Available at <http://mate.dm.uba.ar/~lvendram/rig>.
- [14] M. Graña. Nichols algebras of nonabelian group type, zoo of examples. Available at <http://mate.dm.uba.ar/~matiasg/zoo.html>.
- [15] M. Graña. A freeness theorem for Nichols algebras. *J. Algebra*, 231(1):235–257, 2000.
- [16] I. Heckenberger. The Weyl groupoid of a Nichols algebra of diagonal type. *Invent. Math.*, 164(1):175–188, 2006.
- [17] I. Heckenberger. Classification of arithmetic root systems. *Adv. Math.*, 220(1):59–124, 2009.
- [18] M. Jimbo. A  $q$ -analogue of  $U(\mathfrak{gl}(N+1))$ , Hecke algebra, and the Yang-Baxter equation. *Lett. Math. Phys.*, 11(3):247–252, 1986.
- [19] S. Lang. *Algebra*. Addison-Wesley, 1999.

- [20] A. Milinski and H.-J. Schneider. Pointed indecomposable Hopf algebras over Coxeter groups. In *New trends in Hopf algebra theory (La Falda, 1999)*, volume 267 of *Contemp. Math.*, pages 215–236. Amer. Math. Soc., Providence, RI, 2000.
- [21] W. D. Nichols. Bialgebras of type one. *Comm. Algebra*, 6(15):1521–1552, 1978.
- [22] A. Soloviev. Non-unitary set-theoretical solutions to the quantum Yang-Baxter equation. *Math. Res. Lett.*, 7(5-6):577-596, 2000.
- [23] M. E. Sweedler. *Hopf algebras*. Mathematics Lecture Note Series. W. A. Benjamin, Inc., New York, 1969.
- [24] E. J. Taft. The order of the antipode of finite-dimensional Hopf algebra. *Proc. Nat. Acad. Sci. U.S.A.*, 68:2631–2633, 1971.

M. GRAÑA, DEPARTAMENTO DE MATEMÁTICA, FCEyN, UNIVERSIDAD DE BUENOS AIRES,  
PABELLÓN 1, CIUDAD UNIVERSITARIA (1428), BUENOS AIRES, ARGENTINA  
*E-mail address:* `matiasg@dm.uba.ar`

I. HECKENBERGER, PHILIPPS-UNIVERSITÄT MARBURG, FB MATHEMATIK UND INFORMATIK,  
HANS-MEERWEIN-STRASSE, 35032 MARBURG, GERMANY  
*E-mail address:* `heckenberger@mathematik.uni-marburg.de`

L. VENDRAMIN, DEPARTAMENTO DE MATEMÁTICA, FCEyN, UNIVERSIDAD DE BUENOS AIRES,  
PABELLÓN 1, CIUDAD UNIVERSITARIA (1428), BUENOS AIRES, ARGENTINA

INSTITUTO DE CIENCIAS, UNIVERSIDAD DE GRAL. SARMIENTO, J.M. GUTIERREZ 1150, LOS  
POLVORINES (1653), BUENOS AIRES, ARGENTINA  
*E-mail address:* `lvendramin@dm.uba.ar`